



Универзитет „Св. КИРИЛ И МЕТОДИЈ“ во Скопје
**ФАКУЛТЕТ ЗА ЕЛЕКТРОТЕХНИКА И
ИНФОРМАЦИСКИ ТЕХНОЛОГИИ**

СЕМИНАРСКА РАБОТА

Предмет:

МРЕЖНИ СТАНДАРДИ И УРЕДИ

Тема:

**„DHCP: ОСНОВИ, АРХИТЕКТУРА И
БЕЗБЕДНОСНИ АСПЕКТИ“**

Ментор:

Проф. д-р Данијела Ефнушева

Изработиле:

Ангела Настовска 98/2022

Моника Стоилковска 112/2022

СОДРЖИНА

1. ВОВЕД	4
2. ОСНОВИ НА DHCP	6
2.1. DHCP Компоненти	8
2.2. DHCP ПАКЕТ СТРУКТУРА	10
3. АРХИТЕКТУРА И РАБОТА НА DHCP	12
3.1. DORA	13
3.2. RENEWAL и REBINDING	14
3.3. DHCP RELAY AGENT	15
4. DHCP ВО IPV4 НАСПРОТИ IPV6	16
4.1. РАЗЛИКИ	16
4.2. STATELESS НАСПРОТИ STATEFUL DHCPv6	16
4.3. БЕЗБЕДНОСЕН МОДЕЛ НА IPV6	18
5. ПРЕДНОСТИ НА DHCP	19
6. РАНЛИВОСТ НА DHCP	21
6.1. НЕДОСТАТОЦИ НА АВТЕНТИФИКАЦИЈА	21
6.2. МАНИПУЛАЦИЈА СО DHCP ПАКЕТИ	24
6.3. BROADCAST РАНЛИВОСТ	24
6.4. РАНЛИВОСТ НА НИВО 2	25
7. DHCP НАПАДИ	27
7.1. DHCP НАПАДИ СО ГЛАДУВАЊЕ (STARVATION)	27
7.2. НАПАДИ СО НЕЧЕСЕН DHCP СЕРВЕР	28
7.3. DHCP лажирање (SPOFFING)	29
7.4. DNS киднапирање	31
7.5. Пренасочување на портал	32
7.6. Заробување на сообраќајот	32
8. ТЕХНИКА ЗА ЗАШТИТА НА DHCP	34
8.1. NETWORK ACCESS CONTROL (IEEE 802.1X)	34
8.2. DHCP Шпионирање (SNOOPING)	37
8.3. DYNAMIC ARP INSPECTION – DAI	40
8.4. Заштита на IP извори	42
8.5. Безбедност на порта	43
8.6. VLAN Сегментација	45
8.7. DHCP LEASE TIME	46
8.8. FIREWALL и IDS/IPS мониторинг	48
9. ЗАКЛУЧОК	51

10. КОРИСТЕНА ЛИТЕРАТУРА.....	52
-------------------------------	----

1. Вовед

Во современите компјутерски мрежи, динамичката и автоматизираната конфигурација на уредите претставува основен предуслов за нивната ефикасна, брза и сигурна функционалност. Протоколот **DHCP (Dynamic Host Configuration Protocol)** има клучна улога во овој процес, овозможувајќи автоматско доделување на IP-адреси, subnet маски, default gateway и низа други мрежни параметри кои се неопходни за функционирање на секој мрежен уред. Од домашни рутери, преку корпоративни инфраструктури, па сè до големи центри за податоци, DHCP претставува backbone механизам за конфигурација и одржување на мрежната архитектура. Неговата едноставност, брзина на работа и минимална потреба од човечка интервенција го направија доминантен протокол на глобално ниво.

Сепак, токму оваа едноставност го дефинира и најголемиот проблем на DHCP: тој бил дизајниран во период кога безбедноста не била доминантна димензија во развојот на мрежните технологии. Концептот на доверлива мрежа — каде сите уреди се сметаат за легитимни и безбедни — се покажува како сериозен недостиг во современ контекст, кога заканите се софицирани, напаѓачите се често внатрешни или прикриени, а мрежите се динамични, слоевити и опкружени со потенцијални ризици. Поради ова, во самиот дизајн на DHCP се вградени низа ограничувања и ранливости кои денес претставуваат реална опасност за интегритетот, достапноста и доверливоста на мрежните системи.

Меѓу најкритичните недостатоци се издвојуваат отсуството на механизми за автентификација, употребата на broadcast комуникација и силната зависност од Layer 2 функционалноста, која традиционално е најслабо заштитениот слој во OSI моделот. Овие карактеристики овозможуваат напаѓачите да постават лажни DHCP сервери, да пресретнуваат, изменуваат или инјектираат мрежни конфигурации, како и да иницираат напади кои можат да доведат до целосно прекинување на мрежниот сообраќај. Дополнително, DHCP е подложен на злоупотреба преку техники како DHCP starvation, DHCP spoofing и манипулација со ARP, што ја зголемува комплексноста на заканите и го олеснува изведувањето на „man-in-the-middle“ напади.

Во контекст на организациски мрежи, академски институции и критични инфраструктури, овие ранливости не се само теоретски — тие претставуваат сериозна и практична опасност. Недостатокот од соодветна заштита може да резултира со прекин на услуги, неовластено следење на сообраќајот, мрежна саботажа, пренасочување на податоци кон злонамерни системи, па дури и компромитирање на чувствителни информации. Поради тоа, темелното истражување и разбирање на ранливостите на DHCP претставува важен чекор кон развивање безбедни, стабилни и отпорни мрежни архитектури.

Овој труд има за цел да ги обработи најзначајните аспекти на ранливоста на DHCP, вклучувајќи ги недостатоците на автентификацијата, можностите за манипулација со DHCP пакети, изложеноста што ја создава broadcast комуникацијата и критичните слабости поврзани со Layer 2. Анализата ќе ги опфати техничките механизми, потенцијалните напади, последиците врз мрежната сигурност, како и поширокиот контекст во кој овие ранливости се манифестираат. Со тоа, истражувањето има за цел да обезбеди детален увид во природата на овие закани и да послужи како основа за планирање на адекватни заштитни мерки во современите мрежни системи.

2. Основи на DHCP

Dynamic Host Configuration Protocol (DHCP) е мрежен протокол кој овозможува автоматизирано доделување на мрежни параметри на уредите што се приклучуваат во една TCP/IP мрежа. Неговата основна намена е секој нов уред, без разлика дали станува збор за компјутер, мобилен уред, печатач или IoT систем, да може веднаш да добие валидна IP адреса и други конфигурациски параметри неопходни за комуникација. Со тоа, DHCP ги елиминира сложените, бавни и подложни на грешни процеси на рачна конфигурација, кои во поголемите мрежи би биле практично невозможни.

Во суштина, DHCP претставува автоматски систем за управување со адресниот простор во една мрежа. Протоколот им доделува на уредите IP адреси, маска на подмрежа, default gateway, DNS сервери, време на важност (lease) и други специфични параметри. Овие информации се неопходни за уредот да може успешно да комуницира со други уреди, да пристапува до интернет и да учествува во сите мрежни функции. Без DHCP, мрежниот администратор би морал поединечно да конфигурира секој уред, што би ја зголемило веројатноста за конфликт на IP адреси, погрешни поставки и преоптоварување на администрацијата.

Од архитектонска перспектива, DHCP се наоѓа на **апликацискиот слој** од TCP/IP стекот. Иако формално работи на најгорното ниво, неговото влијание директно се пренесува врз **мрежниот слој**, бидејќи токму DHCP ги дефинира параметрите кои IP протоколот ги користи за адресирање, рутирање и пренос на пакети. Ова го прави DHCP мост помеѓу конфигурациската логика и оперативното функционирање на мрежата.

Дополнително, DHCP тесно соработува со **data-link слојот**, особено во моментите кога уредите сè уште немаат IP адреса и мора да користат broadcast комуникација за да го најдат DHCP серверот. На овој начин, DHCP ја сведува комплексноста на процесите во инфраструктурата на едноставен механизам преку кој уредите без никаква почетна конфигурација можат автоматски да станат дел од мрежниот систем.

Токму поради оваа архитектонска улога, DHCP претставува критичен сервис во секоја модерна мрежа. Тој не само што обезбедува стабилност и конзистентност во конфигурациите, туку овозможува скалабилност, динамичност и ефикасно управување со сите TCP/IP ресурси. Во современите корпоративни, образовни и јавни инфраструктури, DHCP е основа за брзо и сигурно поврзување на уредите, а неговата интеграција е неопходна за правилно функционирање на целиот комуникациски систем.

DHCP во современите компјутерски мрежи претставува суштински елемент на централизираното управување со мрежните конфигурации. Како централизирана

сервисна инфраструктура, DHCP овозможува сите параметри потребни за функционирањето на уредите – IP адреси, мрежни маски, gateway информации, DNS параметри и дополнителни конфигурации – да се контролираат од едно место. Овој модел на работа значително ја поедноставува мрежната администрација, ја зголемува сигурноста и овозможува доследност во конфигурациите низ целата мрежа.

Во централизирана DHCP архитектура, еден или неколку сервери во контролирана средина ја преземаат улогата на управување со адресниот простор за сите мрежни сегменти. Благодарение на овој пристап, мрежните администратори можат точно да ги дефинираат правилата за доделување на ресурси, да спроведат политики за различни типови уреди и да ја следат состојбата на целокупниот адресен пул. Ова централизирано управување не само што го намалува ризикот од IP конфликти и недоследности, туку овозможува и многу поголема контрола врз мрежната безбедност, бидејќи секоја промена, доделување или одбивање на адреса потекнува од еден доверлив извор.

Наспроти централизацијата, децентрализираната DHCP архитектура подразбира повеќе уреди или рутери во мрежата самостојно да извршуваат DHCP функции. Во ваква поставеност секој сегмент или подмрежа може да има свој DHCP сервер кој независно доделува адреси. Иако овој пристап е функционален во мали мрежи со ограничен број уреди, тој брзо станува проблематичен како што мрежата расте. Различните DHCP сервери може да доделуваат преклопени или конфликтни IP опсези, да имаат различни конфигурации или да создадат неконзистентност во DNS и gateway параметрите. Дополнителен ризик е тоа што администраторите немаат преглед над целата мрежа, што ја отежнува дијагностиката и координацијата.

Како резултат на овие ограничувања, децентрализираните модели се сметаат за погодни само во едноставни, локални и малопросторни мрежи, додека сите поголеми и комплексни инфраструктури преферираат централизирано решение. Централизацијата овозможува унифицирани политики, лесно управување со ресурси, central logging за следење активности и подобрена заштита од безбедносни закани.

Потребата од автоматизација е клучен фактор што доведе DHCP да стане доминантно решение во сите модерни мрежи. Во средини каде што бројот на уреди постојано се менува – како што се канцелариски простории, училишта, студентски домови, хотели, производствени системи или јавни Wi-Fi мрежи – рачното конфигурирање на адресите би било практично невозможно. DHCP автоматски обезбедува валидна конфигурација веднаш по поврзување на уредот, без човечка интервенција, што резултира со побрзо приклучување, минимален ризик од грешки и поефективно користење на мрежните ресурси. Автоматизацијата што ја овозможува DHCP го намалува административниот товар, значително го поедноставува одржувањето и овозможува брза адаптација на мрежата на нови услови. На пример, при проширување на мрежата, при додавање нови сегменти или при миграција кон IPv6, DHCP серверот може со неколку промени да обезбеди целосно нова конфигурација за сите уреди. Ова го прави DHCP критично

важен инструмент за скалабилноста и флексибилноста на секоја современа мрежна архитектура.

2.1. DHCP Компоненти

Функционирањето на DHCP се заснова на група меѓусебно поврзани компоненти кои заедно овозможуваат динамична и сигурна распределба на мрежните параметри во TCP/IP околината. Секоја компонента има специфична улога и е неопходна за правилно извршување на процесот на автоматска конфигурација. Основната поставеност на DHCP подразбира постоење на клиент, сервер и ресурси со кои серверот управува, а во поголемите мрежни инфраструктури се вклучува и DHCP relay agent, кој овозможува комуникација меѓу различни подмрежи.

DHCP клиентот претставува уред што бара мрежна конфигурација. Тоа може да биде компјутер, телефон, печатач, камера или било кој друг уред што се приклучува на мрежата без претходно дефинирана IP конфигурација. Клиентот при иницирање на врската започнува комуникациски процес со испраќање на broadcast порака која сигнализира дека му е потребна IP адреса. Во таа фаза уредот сè уште нема сопствена IP адреса, па затоа се потпира на broadcast механизмот за да го пронајде DHCP серверот. Клиентот ја прифаќа конфигурацијата што му ја нуди серверот и ја чува за времетраењето на доделената lease вредност.

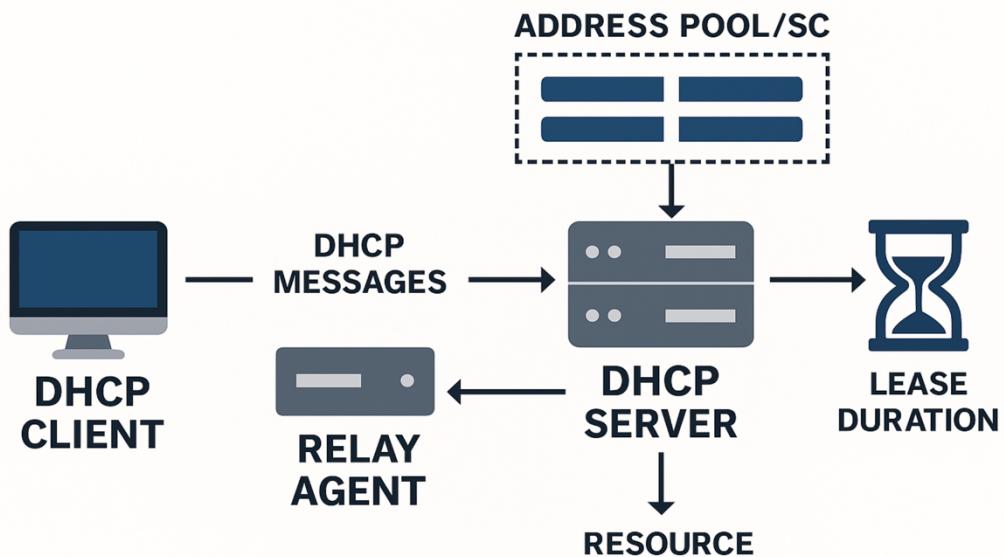
DHCP серверот е централна компонента која управува со целиот процес на распределување на мрежните параметри. Серверот располага со база на расположливи IP адреси и со низа дополнителни параметри кои можат да им бидат доделени на клиентите. Во инфраструктурите со поголем број уреди, серверот е конфигуриран со различни политики, резервирани адреси, специфични параметри за одделни групи уреди и правила кои го регулираат времетраењето на lease механизмот. Кога клиентот ќе испрати барање, серверот избира слободна адреса од својот адресен опсег и ја нуди на клиентот заедно со сите неопходни параметри: маска на подмрежа, default gateway, DNS сервери и други опционални информации. Серверот, исто така, го следи кои адреси се активни, кои се истечени и кои уреди се поврзани во даден момент.

Во ситуации кога клиентот и серверот се наоѓаат во различни подмрежи, директната комуникација преку broadcast не е можна, бидејќи рутерите не ги пропуштаат broadcast пакетите поради ограничувањата на нивната архитектура. Тука се користи DHCP relay agent, кој ја прима broadcast пораката од клиентот и ја пренесува кон серверот користејќи unicast комуникација. Relay agent овозможува еден централен DHCP сервер да управува со повеќе географски или логички разделени мрежни сегменти, без потреба во секоја подмрежа да постои посебен DHCP сервер. Ова ја подобрува ефикасноста, го намалува бројот на уреди што треба да се одржуваат и ги елиминира проблемите со недоследни конфигурации.

Address pool или scope претставува дефиниран опсег на IP адреси со кои DHCP серверот управува. Овој пул е логички организирана група адреси кои се резервирали за динамична доделба. Администраторот може да дефинира повеќе пулови за различни VLAN-и, подмрежи или категории на уреди. Scope-от може да содржи адреси што се достапни за динамична доделба, резервирали адреси за специфични уреди врз основа на нивната MAC адреса или исклучени опсези што серверот никогаш не смее да ги додели. Со ова, DHCP серверот овозможува прецизна контрола на мрежниот адресен простор.

Lease duration е временскиот период за кој клиентот смее да ја користи доделената IP адреса. Ова време може да биде кратко, како неколку минути или часови, како што е во јавните Wi-Fi мрежи, или многу долго, како неколку дена или недели, во стабилни корпоративни мрежи со постојани уреди. Lease механизмот овозможува динамично ослободување и повторно користење на IP адресите кога уредите престануваат да бидат активни. Клиентот е одговорен да го обнови својот lease пред истекот, а серверот решава дали ќе го продолжи или ќе му додели нова адреса доколку постојат промени во мрежната политика (Слика 1).

Користењето на DHCP ресурсите овозможува оптимално управување со адресниот простор, автоматско распределување на конфигурациите и поддршка на големи динамични системи. Благодарение на овие компоненти, DHCP функционира како потполно автоматизиран систем кој овозможува стабилност, скалабилност и сигурност во секоја модерна мрежна архитектура.



Слика 1. Основни DHCP компоненти

2.2. DHCP пакет структура

DHCP комуникацијата се базира на стандардизирана структура на пакети која потекнува од постариот BOOTP протокол, но е проширена за да поддржи динамичко конфигурирање и голем број дополнителни параметри. Секоја DHCP порака се пренесува преку UDP транспортниот протокол, при што клиентите користат порта 68, а серверите порта 67. DHCP пакетот има фиксна основна форма, составена од хедер со строго дефинирани полиња и сегмент за опции кој претставува најфлексибилниот дел на пакетот. Ова овозможува и основна идентификација на клиентот без IP адреса, и пренесување на целосна конфигурација преку еден централен протокол.

Во основната структура на DHCP пакетот хедерот претставува централниот дел кој ги содржи сите информации неопходни за контролирање на процесот на доделување на адреси. Првото поле, означеното како *op*, ја дефинира природата на пораката и означува дали пакетот претставува барање од клиентот или одговор од серверот. Потоа следат полињата *htype* и *hlen*, кои укажуваат на типот на хардверската адреса и нејзината должина, најчесто со вредности поврзани со Ethernet адаптерите. Значајно поле е *hops*, кое се користи од DHCP relay agent кога пакетот мора да помине низ повеќе рутери за да стигне до DHCP серверот.

Еден од најважните елементи на DHCP хедерот е *transaction ID (xid)*, уникатен 32-битов број генериран од клиентот. Овој идентификатор овозможува серверот да ги поврзе сите пораки што се однесуваат на истата комуникациска сесија и да разликува паралелни барања од различни клиенти. Ова е особено важно затоа што DHCP комуникацијата започнува кога клиентот нема IP адреса и затоа серверот мора да го идентификува клиентот преку механизми кои не зависат од IP ниво.

Покрај идентификаторите, хедерот содржи повеќе полиња што ја дефинираат IP адресата која се бара или која се нуди. Полето *ciaddr* содржи IP адреса која клиентот веќе ја има и ја обновува, додека *yiaddr* (your IP address) ја претставува IP адресата што серверот ја предлага на клиентот. Полето *siaddr* укажува на адресата на серверот што може да се користи за boot услуги, а *giaddr* ја содржи IP адресата на relay агентот кога пакетот е препратен преку друг мрежен сегмент. Многу важно поле е *chaddr*, во кое се чува MAC адресата на клиентот. Ова е единствената сигурна идентификација на уредот во фазата кога тој сè уште нема IP адреса.

Полето за опции, кое се наоѓа по фиксниот хедер, претставува најмоќниот и најдинамичен дел од DHCP пакетот. DHCP options содржат низа параметри што серверот може да ги испрати до клиентот, а кои ги дефинираат сите аспекти на мрежната конфигурација. Преку нив се испраќаат информациите за subnet mask, default gateway, DNS серверите, траењето на lease периодот, доменските параметри, статичките рутери и многу други специјализирани вредности.

Меѓу најважните опции е *DHCP Message Type*, која укажува дали пакетот е DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK, DHCPNAK или друг тип порака. Оваа опција ја дефинира логиката на комуникацијата и овозможува правилно следење на секој чекор во процесот на доделување адреси. Друг критичен елемент е *Server Identifier*, преку кој клиентот може јасно да знае од кој DHCP сервер потекнува понудата, особено кога повеќе сервери се присутни во мрежата. Опциите како *Lease Time*, *Renewal Time (T1)* и *Rebinding Time (T2)* ја дефинираат валидноста на доделените параметри и процесот на нивно обновување.

Бидејќи DHCP options овозможуваат протоколот да биде флексибilen, тој може да се користи не само за основна IP конфигурација, туку и за специјализирани задачи како PXE booting, автоматска конфигурација на VoIP телефони, TFTP информации и политики за различни категории уреди. Со ова, DHCP станува не само механизам за доделување адреси, туку систем за централизирано управување со мрежната инфраструктура (Слика 2).

DHCP Packet Format			
Operation Code	Hardware Type	Hardware Length	Hop Count
Transition ID			
Number of Seconds		Flags	
Client IP Address			
Your IP Address			
Server IP Address			
Gateway IP Address			
Client Hardware Address (16 Byte)			
Server Name (64 Byte)			
Boot File Name (128 Byte)			
Option (Variable Length)			

Слика 2. Пакет структура на DHCP

3. Архитектура и работа на DHCP

Архитектурата на DHCP се базира на централизирано управување со мрежната конфигурација и динамичка размена на пораки помеѓу клиентот и серверот. Основниот принцип на работа е дека клиентот, при негово приклучување во мрежата, не поседува IP адреса и затоа мора да комуницира преку DHCP за да добие валидни мрежни параметри. Целиот процес е структуриран така што DHCP обезбедува автоматско, сигурно и контролирано доделување на адреси, со што ја поедноставува администрацијата и го намалува ризикот од конфликти.

Комуникацијата помеѓу клиентот и серверот се одвива преку стандарден механизам познат како DORA процес, кој вклучува четири главни фази: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST и DHCPACK. Овој процес претставува основниот механизам преку кој клиентот ја иницира својата потреба за конфигурација, серверот нуди адреса, клиентот ја прифаќа, а серверот ја потврдува завршената доделба. DORA циклусот е фундаментален дел од архитектурата на DHCP, бидејќи гарантира дека секој уред добива уникатна адреса и валидни параметри во моментот кога му се потребни. Овој процес често се прикажува со графички дијаграм за полесно разбирање на редоследот на пораките.

Откако уредот ќе добие IP адреса, неговата конфигурација не е трајна, туку има ограничено времетраење познато како lease. За да се одржи валидна конективност, DHCP архитектурата вклучува механизми за автоматско обновување на адресата, преку што клиентот периодично бара продолжување. Овој процес е регулиран преку два тајмера, означени како T1 и T2, со кои се определува моментот кога клиентот треба да се обиде да ја обнови адресата кај оригиналниот сервер, и моментот кога мора да побара обновување од било кој DHCP сервер достапен во мрежата. На овој начин се обезбедува стабилност и непречено функционирање дури и во ситуации кога серверот може привремено да биде недостапен.

Во многу мрежи DHCP серверот и клиентот не се наоѓаат во истата подмрежа, што претставува технички предизвик, бидејќи DHCP комуникацијата во првичната фаза се заснова на broadcast пораки, кои не поминуваат преку рутери. За да се реши овој проблем, архитектурата на DHCP вклучува DHCP relay agent, кој има задача да ги пренесува DHCP пораките меѓу различни мрежни сегменти. Relay агентот ја прима broadcast пораката од клиентот во локалниот сегмент и ја препраќа како unicast кон DHCP серверот во друг сегмент, користејќи UDP пренос. Со ова се овозможува централизираниот DHCP сервер да ги опслужува сите подмрежи во една организација, без да се поставува посебен сервер во секој сегмент.

Со поврзувањето на основниот DORA процес, механизмите за обновување на адресите и улогата на relay агентите, архитектурата на DHCP станува целосно функционален систем што овозможува скалабилно, сигурно и автоматизирано

управување со мрежните параметри во комплексни инфраструктури. Сите следни подточки детално ги разработуваат овие процеси.

3.1. DORA

Основниот механизам преку кој DHCP ги доделува мрежните параметри на клиентските уреди е DORA процесот, кој го носи името по иницијалите на четирите последователни пораки што се разменуваат помеѓу клиентот и серверот: Discover, Offer, Request и Acknowledgement. DORA (Слика 3) претставува централен дел од архитектурата на DHCP и ја дефинира целокупната комуникација нуждна за автоматско доделување на IP адреси.

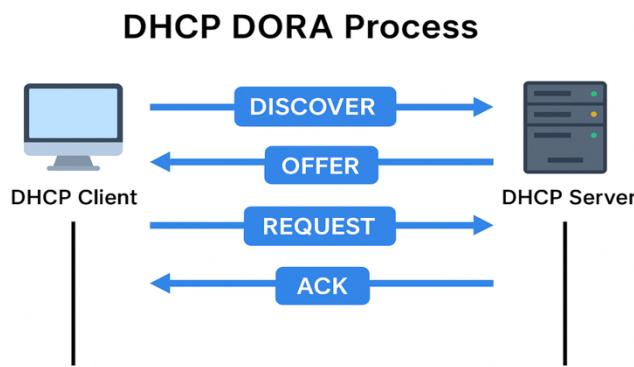
Процесот започнува со фазата *Discover*, кога клиентот, кој се приклучува на мрежата и сè уште нема IP адреса, испраќа broadcast порака со која бара DHCP сервер. Оваа порака е испратена како broadcast затоа што клиентот технички не знае каде се наоѓа серверот и зависи од тоа сите сервери во локалниот сегмент да ја примат.

Следната фаза е *Offer*, во која еден или повеќе DHCP сервери реагираат на Discover пораката и му испраќаат на клиентот понуда што содржи IP адреса од нивниот address pool, заедно со дополнителни параметри како мрежна маска, gateway и DNS сервер. Клиентот може да добие повеќе понуди, но ќе избере само една од нив.

Третиот чекор е *Request*, каде клиентот испраќа порака со која потврдува дека ја прифаќа понудата од конкретен DHCP сервер. Иако комуникацијата е broadcast, оваа порака содржи информации за тоа кој сервер е избран, со што другите сервери што испратиле понуда знаат дека нивните адреси не треба да се резервираат за овој клиент.

Процесот завршува со *ACK* (Acknowledgement), односно потврдата што серверот ја испраќа до клиентот за да ја формализира доделбата на IP адресата. Во оваа порака се испорачуваат сите конечни параметри, вклучувајќи го и времетраењето на lease периодот. Од овој момент клиентот има валидна мрежна конфигурација и може целосно да учествува во TCP/IP комуникацијата.

DORA процесот е дизајниран така што обезбедува сигурна и контролирана размена на информации, избегнувајќи IP конфликти и дозволувајќи на серверот да има точна евиденција за кои адреси се зафатени.



Слика 3. DORA Процес

3.2. Renewal и Rebinding

Откако DHCP клиентот ќе добие IP адреса од серверот, таа адреса не е трајна, туку има ограничено времетраење наречено *lease time*. Lease времето одредува колку долго клиентот може да ја користи доделената адреса пред да мора да ја обнови. Овој механизам обезбедува динамично управување со IP адресниот простор, така што неактивните или исклучените уреди не „задржуваат“ адреси непотребно.

Процесот на обновување на lease времето е целосно автоматизиран и се спроведува преку два важни тајмера: T_1 и T_2 . Тајмерот T_1 претставува период во кој клиентот започнува тивка, директна комуникација со DHCP серверот од кој првично ја добил адресата. Обично T_1 е поставен на 50% од вкупното lease време. На пример, ако IP адресата важи 24 часа, T_1 ќе се активира по 12 часа. Во оваа фаза клиентот испраќа DHCPREQUEST порака директно до серверот, со цел да го продолжи користењето на истата адреса. Ако серверот е достапен и ја прифаќа барањето, тој испраќа DHCPACK порака и lease периодот се обновува без било каков прекин во функционирањето на клиентот.

Доколку серверот не одговори во T_1 периодот — што може да се случи поради привремени мрежни проблеми, преоптовареност или прекин на услугата — клиентот влегува во втората фаза, дефинирана со тајмерот T_2 . Овој тајмер е најчесто поставен на 87.5% од lease времето. Во T_2 фазата, клиентот веќе не се обидува да комуницира само со оригиналниот DHCP сервер, туку испраќа broadcast DHCPREQUEST до сите можни DHCP сервери во мрежата. Ова значи дека клиентот бара обновување од „било кој“ сервер кој е достапен и овластен да издава адреси за тој сегмент. T_2 е критичен механизам што спречува целосно губење на конекцијата во ситуации кога оригиналниот сервер е недостапен, а мрежата има резервни DHCP сервери или failover конфигурации.

Ако и по истекот на T_2 клиентот не добие DHCPACK, тогаш адресата влегува во состојба на *expiration*. Во овој момент клиентот ја губи валидноста на IP адресата и мора повторно да го започне целиот DORA процес за да добие нова конфигурација. Овој механизам спречува уредите да користат адреси кои повеќе не се валидни или пак припаѓаат на друг subnet по мрежна реорганизација.

Обновувањето и rebinding механизмите овозможуваат DHCP да обезбеди стабилност, континуирана конективност и автоматска адаптација, без уредите да мораат да губат своето мрежно поврзување. Со ова DHCP станува протокол кој се грижи уредите секогаш да располагаат со валидна IP конфигурација, дури и во динамични и променливи мрежни средини.

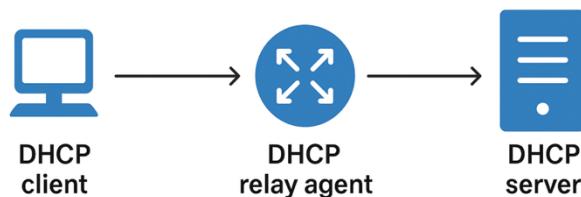
3.3. DHCP Relay Agent

Во основната форма на DHCP, комуникацијата помеѓу клиентот и серверот се заснова на broadcast пораки, особено во почетната фаза кога клиентот сè уште нема IP адреса. Broadcast пакетите, по својата природа, се ограничени на локалниот мрежен сегмент и не можат да поминуваат преку рутери. Ова претставува проблем во поголеми и посложени мрежи кои се поделени на повеќе подмрежи (subnets), бидејќи DHCP серверот најчесто се наоѓа централизирано, а клиентите се распоредени низ различни сегменти.

За да се надмине ова ограничување, во DHCP архитектурата се користи компонентата наречена *DHCP relay agent*. Relay агентот обично е имплементиран на рутер или Layer 3 switch и има задача да ги пренесува DHCP пораките помеѓу клиентите и DHCP серверот, дури и кога тие се наоѓаат во различни мрежни сегменти. Кога клиентот испраќа DHCPDISCOVER broadcast порака во својот локален сегмент, relay агентот ја пресретнува таа порака и ја препраќа како unicast порака директно до DHCP серверот. На тој начин се овозможува комуникација без потреба серверот физички да биде присутен во секоја подмрежа.

Relay агентот, при препраќањето на пораките, ја пополнува и специјалната информација за изворниот мрежен сегмент, најчесто преку *giaddr* (gateway IP address) полето во DHCP пораката. Ова му овозможува на DHCP серверот да знае од кој subnet доаѓа барањето и да додели IP адреса од соодветниот address pool или scope. Серверот потоа ја испраќа својата понуда назад до relay агентот, кој ја препраќа до клиентот, најчесто како broadcast во локалниот сегмент на клиентот. Комуникацијата помеѓу клиентот, relay агентот и серверот се одвива преку UDP протоколот, користејќи ги стандардните порти 67 (DHCP сервер) и 68 (DHCP клиент). UDP е избран поради неговата едноставност и мала латентност, што е соодветно за иницијална конфигурација на уредите. Сепак, бидејќи UDP не обезбедува вградена сигурност и контрола на испораката, DHCP мора да користи сопствени механизми за повторување на пораките и временски ограничувања.

Употребата на DHCP relay agent овозможува централизирано управување со IP адресирањето и значително ја поедноставува мрежната архитектура, бидејќи нема потреба од поставување DHCP сервер во секој сегмент. Истовремено, ова решение ги почитува ограничувањата на broadcast комуникацијата и овозможува скалабилност, што го прави DHCP применлив и во големи корпоративни и кампус мрежи.



Слика 4. Функција на DHCP Relay Agent

4. DHCP во IPv4 наспроти IPv6

DHCP протоколот постои и во IPv4 и во IPv6 мрежите, но неговата улога и начинот на функционирање се разликуваат поради фундаменталните разлики меѓу двата IP протоколи. Во IPv4 мрежите, DHCP има централна улога во целосната конфигурација на уредите, бидејќи без него клиентот не може автоматски да добие IP адреса и основни мрежни параметри. IPv4 адресниот простор е ограничен, што ја прави динамичката распределба преку DHCP особено важна за ефикасно користење на достапните адреси.

Во IPv6 мрежите, DHCP има поинаква и понекогаш дополнителна улога. IPv6 е дизајниран со значително поголем адресен простор и поддржува механизам за автоматска конфигурација наречен Stateless Address Autoconfiguration (SLAAC). Со SLAAC, уредите можат самостојно да креираат IPv6 адреса без директна интеракција со DHCP сервер. Поради ова, DHCP во IPv6 не е секогаш задолжителен за доделување IP адреси, туку често се користи за доставување дополнителни информации како DNS сервери, domain name или други мрежни параметри.

4.1. Разлики

Значајна разлика е начинот на комуникација. DHCPv4 интензивно користи broadcast пораки, особено во почетната фаза на DORA процесот. Наспроти тоа, DHCPv6 не користи класичен broadcast, туку multicast комуникација, што е поефикасно и подобро прилагодено за модерни мрежи. Исто така, DHCPv6 работи со различни UDP порти и има поинаква структура на пораките во споредба со DHCPv4.

Дополнително, во IPv6 мрежите, улогата на рутерите е значително поголема. Router Advertisement (RA) пораките му кажуваат на клиентот дали треба да користи SLAAC, DHCPv6 или комбинација од двата механизми. Ова овозможува поголема флексибилност, но и поголема комплексност во дизајнот и управувањето со мрежата.

Сумирено, DHCP во IPv4 претставува основен и задолжителен механизам за автоматска мрежна конфигурација, додека во IPv6 тој е дел од поширок систем за конфигурација, кој комбинира повеќе технологии со цел поголема скалабилност, ефикасност и флексибилност.

4.2. Stateless наспроти Stateful DHCPv6

Во IPv6 мрежите, конфигурацијата на уредите може да се реализира преку два различни пристапи: stateless и stateful, кои се дефинирани според начинот на кој се управува со IP адресите и мрежните параметри. Овие два модели нудат различно ниво

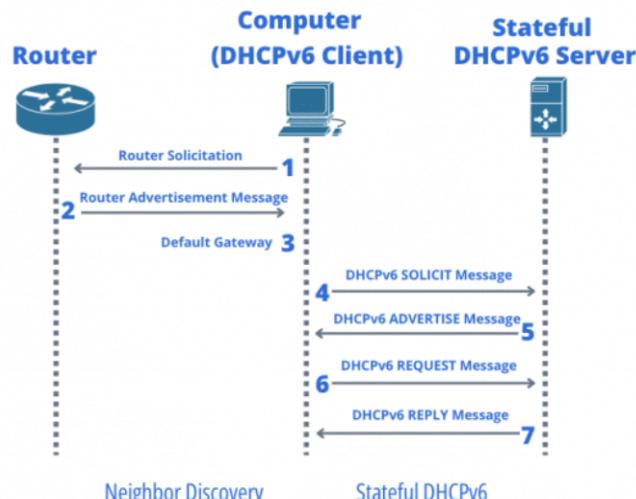
на контрола и автоматизација и се користат во зависност од потребите и политиките на мрежата.

Stateful DHCPv6 функционира на сличен начин како традиционалниот DHCP во IPv4 мрежите. Во овој модел, DHCP серверот има целосна контрола врз доделувањето на IPv6 адресите и води детална евиденција за секој клиент, вклучувајќи ја доделената адреса, времетраењето на lease периодот и идентитетот на уредот. Клиентот добива IP адреса директно од DHCPv6 серверот, заедно со сите потребни мрежни параметри. Овој пристап овозможува централизирано управување, прецизна контрола и лесно следење на уредите во мрежата, што е особено важно во корпоративни и контролирани околини.

Stateless DHCPv6, од друга страна, не учествува во директното доделување на IP адреси. Наместо тоа, клиентите самостојно ја креираат својата IPv6 адреса преку механизмот Stateless Address Autoconfiguration (SLAAC), користејќи информации добиени од Router Advertisement пораките. DHCPv6 во овој случај служи исклучиво за доставување дополнителни мрежни параметри, како што се DNS сервери, доменско име или други опции. Серверот не води евиденција за доделените IP адреси, што значи дека не постои состојба (state) за адресирањето на клиентите.

Главната разлика меѓу двата пристапи лежи во нивото на контрола. Stateful DHCPv6 овозможува централизирана и детерминистичка распределба на адреси, додека stateless пристапот нуди поголема флексибилност и автоматизација со помала административна сложеност. Изборот помеѓу stateless и stateful зависи од потребите на мрежата, безбедносните барања и степенот на управување што администраторот сака да го задржи врз адресниот простор.

Во пракса, овие два механизми често се користат и во комбинација, каде што SLAAC се користи за адресирање, а stateless DHCPv6 за доставување на дополнителни параметри. Ова овозможува баланс помеѓу автоматизација и контрола, што е една од клучните предности на IPv6 мрежите.



Слика 5. Како работи Stateful DHCPv6

4.3. Безбедносен модел на IPv6

Воведувањето на IPv6 не претставува само проширување на адресниот простор, туку значително го менува и безбедносниот модел на мрежите. За разлика од IPv4, каде што безбедноста често се имплементира дополнително и селективно, IPv6 е дизајниран со вградени безбедносни механизми и поинаква логика на комуникација, што влијае директно врз начинот на кој функционираат протоколите за конфигурација како DHCPv6.

Една од клучните промени е задолжителната поддршка за IPsec во IPv6. Иако IPsec не мора секогаш да биде активен, неговата интеграција во стандардот ја нагласува ориентацијата кон повисоко ниво на безбедност на мрежно ниво. Ова создава можност за автентификација и енкрипција на сообраќајот, што е особено важно во мрежи каде што DHCPv6 се користи за дистрибуција на чувствителни параметри како DNS сервери и политики за рутирање.

IPv6 исто така го елиминира класичниот broadcast сообраќај, кој во IPv4 претставуваше значајна површина за напади. Наместо тоа, IPv6 користи multicast комуникација, што овозможува поефикасна и поконтролирана дистрибуција на пораките. Иако multicast не е целосно имун на злоупотреби, тој значително ја намалува изложеноста на мрежата на масовни broadcast-базирани напади, вклучувајќи и некои типови на DHCP злоупотреби.

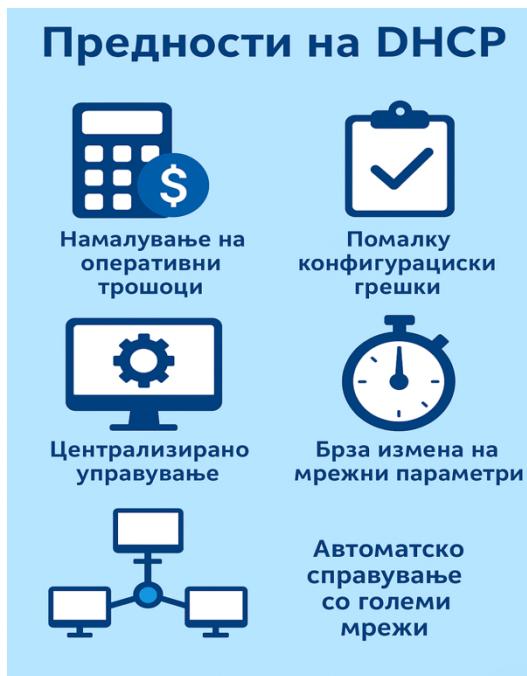
Дополнително, во IPv6 мрежите, улогата на Router Advertisement (RA) пораките станува критична. Клиентите се потпираат на овие пораки за да одлучат дали ќе користат SLAAC, stateful DHCPv6 или stateless DHCPv6. Ова го проширува безбедносниот модел, бидејќи напаѓачите можат да таргетираат RA пораки со цел да манипулираат со мрежната конфигурација. Поради тоа, IPv6 воведува потреба од дополнителни механизми за заштита како RA Guard и Secure Neighbor Discovery (SeND).

Исто така, огромниот адресен простор на IPv6 ја менува стратегијата за скенирање и откривање на уреди во мрежата. Додека во IPv4 нападите често се базираат на систематско скенирање на цел subnet, во IPv6 ова станува значително потешко. Ова индиректно ја подобрува безбедноста, но истовремено бара нови алатки и пристапи за мониторинг и детекција на закани.

Сумирано, IPv6 воведува поинаков безбедносен модел кој комбинира вградени заштитни механизми, нови типови комуникација и зголемена комплексност. Во тој контекст, DHCPv6 мора да се разгледува како дел од поширок безбедносен екосистем, каде што заштитата не зависи само од еден протокол, туку од правилната интеграција на повеќе технологии и политики.

5. Предности на DHCP

Една од најзначајните предности на користењето на DHCP (Dynamic Host Configuration Protocol) во современите компјутерски мрежи е значителното **намалување на оперативните трошоци** поврзани со администрацијата и одржувањето на мрежната инфраструктура. Во мрежи каде што IP адресите и другите мрежни параметри се конфигурираат рачно, потребно е значително време и човечки ресурси за правилно доделување, следење и ажурирање на конфигурациите за секој уред поединечно. DHCP ја елиминира оваа потреба преку автоматизирано доделување на IP адреси, subnet маски, default gateway и DNS сервери, со што се намалува оптоварувањето на систем администраторите и се оптимизира користењето на ресурсите.



Слика 6. Дел од предностите на DHCP

Автоматизацијата што ја нуди DHCP директно придонесува и за **намалување на конфигурациските грешки**, кои се честа појава при рачна конфигурација. Грешки како дуплирани IP адреси, погрешна subnet маска или неточен gateway можат да доведат до сериозни проблеми во комуникацијата и достапноста на мрежните услуги. Со централизирано дефинирани правила и параметри на DHCP серверот, сите клиенти добиваат конзистентна и проверена конфигурација, што значително ја зголемува стабилноста и доверливоста на мрежата.

Дополнително, DHCP овозможува **централизирано управување** со мрежните конфигурации, што е особено важно во средни и големи организации. Наместо промените да се вршат на секој уред поединечно, администраторот може да направи измена само на DHCP серверот, а таа автоматски ќе се примени на сите клиенти при следното обновување на lease-от. Овој пристап овозможува подобра контрола, полесно следење на доделените IP адреси и поефикасно решавање на проблеми.

DHCP исто така овозможува **брза и флексибилна измена на мрежните параметри**, што е клучно во динамични мрежни околини. Промени како замена на DNS сервери, промена на gateway или адаптација на мрежната структура може да се извршат без потреба од физички пристап до клиентските уреди. Ова значително ја намалува времето потребно за имплементација на промени и го минимизира прекинот на работата на корисниците.

Конечно, една од најважните предности на DHCP е неговата способност за **автоматско справување со големи и комплексни мрежи**. Во средини со голем број уреди, како што се универзитети, компании или јавни мрежи, рачната IP конфигурација е практично невозможна и неефикасна. DHCP овозможува динамично управување со address pool-ови, оптимално користење на IP адресниот простор и лесна поддршка на мобилни и привремени уреди кои често се приклучуваат и исклучуваат од мрежата. Со тоа, DHCP претставува клучна компонента за скалабилноста, ефикасноста и стабилноста на модерните мрежни системи.

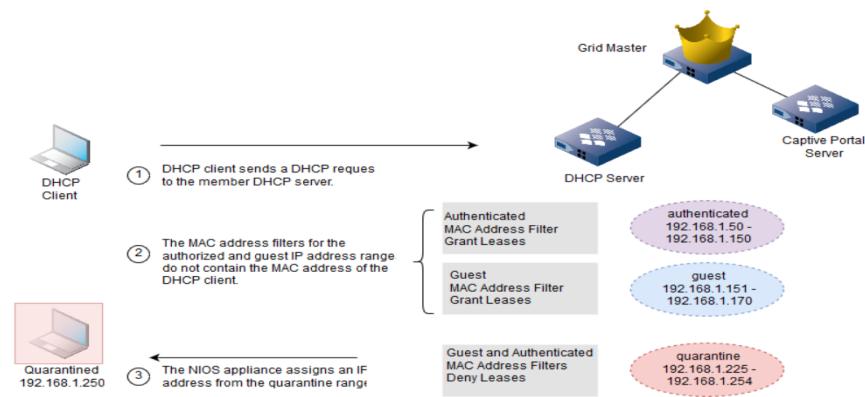
6. Ранливост на DHCP

Динамичкиот протокол за конфигурација на хостови (DHCP) претставува еден од клучните мрежни сервиси кој овозможува автоматска распределба на IP адреси и други мрежни параметри кон уредите во една локална мрежа. Благодарение на овој протокол, администрацијата на мрежите станува значително поедноставна, а комуникацијата помеѓу уредите побрза и поефикасна. Сепак, токму поради неговата автоматизирана природа и доверливиот модел на функционирање, DHCP претставува цел на бројни безбедносни закани. Ранливостите кои произлегуваат од недоволна автентификација, отсуството на енкрипција и можноста за манипулација со DHCP пораките создаваат простор за напади како DHCP spoofing, rogue DHCP сервери и MAC flooding. Овие напади можат сериозно да ја нарушат безбедноста и стабилноста на мрежата, доведувајќи до пренасочување на сообраќај, прекин на услуги или целосно преземање на мрежната комуникација. Следствено анализата на ранливост во DHCP протоколот е од суштинско значење за секој безбедносен аналитичар и мрежен администратор. Разбирањето на начинот на кој функционира овој протокол, заедно со методите на напад и заштита, овозможува навремено препознавање на ризиците и имплементација на соодветни безбедносни механизми.

6.1. Недостатоци на автентификација

Најкритичната и фундаментална ранливост на Dynamic Host Configuration Protocol (DHCP) произлегува од фактот дека протоколот е дизајниран без никаков механизам за автентификација ниту помеѓу клиентот и серверот, ниту помеѓу самите DHCP сервери.

Овој протокол функционира врз принципот на доверба, односно секој уред кој испраќа DHCP барање во мрежата се смета за валиден клиент, а секој одговор што пристигнува до клиентот се прифаќа како легитимен DHCP сервер. Отсуството на можност за проверка на идентитетот овозможува напаѓачот лесно да се претстави како легитимен DHCP сервер и да испраќа лажни конфигурациски параметри. DHCP автентификацијата се базира на споделен таен клуч помеѓу DHCP серверот и клиентот. Клучот се користи за генерирање на код за автентификација на пораки (MAC) кој се додава на DHCP пораките. MAC го потврдува идентитетот и интегритетот на испраќачот и примачот на пораките. MAC исто така спречува напади со повторно прикажување, каде што напаѓачот снима и повторно



Слика 7. Сместување во карантин на неафентифициран DHCP клиент

пренесува валидна DHCP порака за да добие неовластен пристап или да предизвика одбивање на услугата.

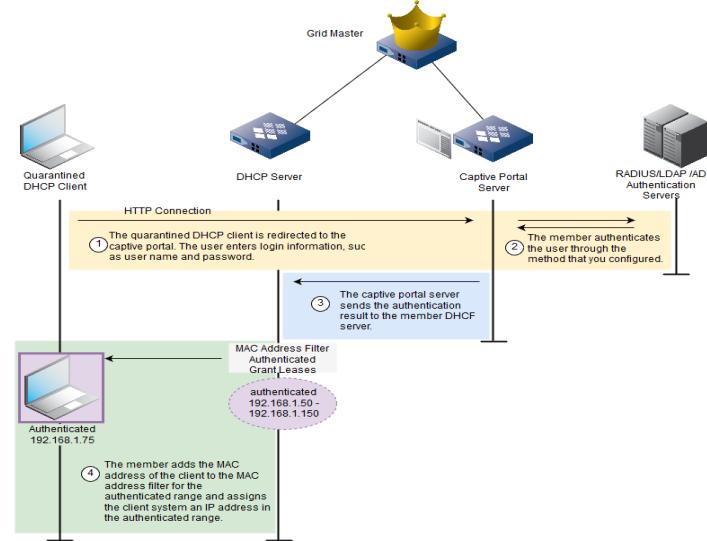
Како што е прикажано на Слика 7, процесот на автентикација во DHCP започнува кога DHCP клиентот ќе се обиде да се приклучи на мрежата. Додека DHCP сервер проверува дали MAC адресата на DHCP клиентот се совпаѓа со некоја од MAC адресите наведени во филтрите за гости или автентицирани MAC адреси. Доколку серверот не пронајде совпаѓање, на клиентот му доделува IP адреса од карантинскиот опсег. Кога клиентот ќе се обиде да пристапи до веб-страница, тој се пренасочува кон captive portal страницата. Треба да се напомене дека карантинскиот опсег во Слика 1 содржи MAC филтри кои спречуваат доделување на IP адреси од тој опсег на DHCP клиенти чија MAC адреса се совпаѓа со некоја од адресите во филтрите за гости или автентицирани корисници. Кога клиентот преку веб-предстувац ќе се поврзе со IP адресата на captive portal страницата, корисникот може да се регистрира и да го продолжи процесот на автентикација за да добие IP адреса од опсегот за автентицирани корисници, или да се регистрира како гостин и да добие IP адреса од гостинскиот DHCP опсег. Доколку

корисникот избере да го продолжи процесот на автентикација, како што е прикажано на Слика 2, DHCP серверот го автентицира корисникот преку автентикацискиот сервис кој е конфигуриран, а тоа може да биде RADIUS, LDAP или Active Directory (AD).

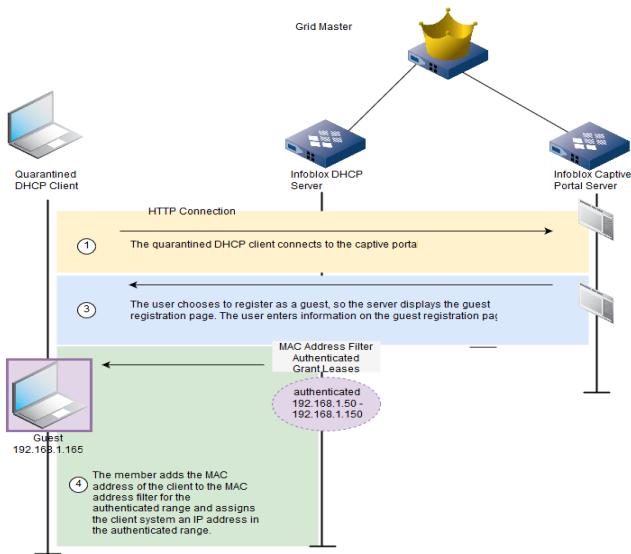
Откако клиентот успешно ќе го помине процесот на автентикација, уредот ја складира неговата MAC адреса во филтерот за MAC адреси кој се однесува на опсегот за автентицирани корисници. Кога клиентот ќе се обиде да ја обнови својата IP адреса, тој добива нова IP адреса од DHCP опсегот наменет за автентицирани клиенти.

Треба да се напомене дека ако филтерот за MAC адреси има дефиниран период на истекување, системот автоматски ги брише истечените MAC адреси од филтерот. Поради тоа, доколку DHCP клиент се обиде да ја обнови својата IP адреса по истекот на овој период, клиентот повторно се пренасочува кон captive portal страницата, бидејќи неговата MAC адреса повеќе не е присутна во филтерот.

Откако корисникот ќе се најави како гостин, уредот ја зачувува MAC адресата на клиентот во филтерот за MAC адреси кој се однесува на гостинскиот опсег. Кога DHCP



Слика 8. Автентификација на корисник



Слика 9. Регистрација како гостин

клиентот ќе се обиде да ја обнови својата IP адреса, тој добива нова IP адреса од гостинскиот DHCP опсег, освен во случај кога MAC адресата на клиентот истекла и била отстранета од филтерот. Во таква ситуација, DHCP клиентот повторно се пренасочува кон captive portal страницата.

DHCP автентикацијата обезбедува значајни придобивки за безбедноста и управувањето на мрежата. Прво, таа го спречува пристапот на неовластени клиенти кон IP адресите и мрежните ресурси, што значително го намалува ризикот од преоптоварување на мрежата, конфликти на IP адреси и напади со лажирање. Второ, DHCP

автентикацијата го спречува дејствувањето на лажни DHCP сервери кои би можеле да им нудат погрешни конфигурациски параметри на клиентите, со што се избегнува пренасочување кон злонамерни веб-страници, прокси-сервери или портали. Трето, таа овозможува на мрежниот администратор да ја следи и ревидира активноста на DHCP и да спроведува политики врз основа на идентификацијата и атрибутите на клиентите, обезбедувајќи контролиран и сигурен мрежен сообраќај.

DHCP автентикацијата, исто така, има некои предизвици и ограничувања. Таа бара безбеден и сигурен начин за дистрибуција и управување со клучевите. Ако клучевите се компромитирани, украдени или изгубени, DHCP автентикацијата ќе не успее или ќе биде заобиколена. Второ, таа бара клиентите да го поддржуваат протоколот и опциите за DHCP автентикација. Не сите уреди и оперативни системи поддржуваат DHCP автентикација, особено постарите или застарените. Трето, таа не ги шифрира DHCP пораките, туку само ги автентицира. Пораките сè уште можат да бидат пресретнати и прочитани од напаѓач, откривајќи чувствителни информации како што се имиња на хостови, MAC адреси и времиња на закуп.

За да ја подобрите DHCP автентикацијата, можете да користите некои дополнителни мерки и најдобри практики. Прво, можете да користите безбеден и централизиран систем за управување со клучеви што може да генерира, дистрибуира, складира, ротира и поништува клучеви. Исто така, можете да користите различни клучеви за различни опсези, групи или класи на клиенти за да го ограничите влијанието на компромитирање на клуч. Второ, можете да користите заштитен сид или листа за контрола на пристап за да го филтрирате DHCP сообраќајот и да дозволите само овластениот DHCP сервер и клиенти да комуницираат. Исто така, можете да користите функција за безбедност на портата на прекинувачот за да ги поврзете MAC адресите со портите на прекинувачот и да спречите неовластени уреди да се поврзат со мрежата.

Трето, можете да користите VPN или протокол за шифрирање за да ги шифрирате DHCP пораките и да ги заштитите од прислушување и неовластено ракување.

6.2. Манипулација со DHCP пакети

Манипулацијата со DHCP пакети претставува процес на менување или неправилно обработување на информациите што се разменуваат помеѓу DHCP клиентот и DHCP серверот. DHCP протоколот функционира преку серија пакети (DISCOVER, OFFER, REQUEST, ACK), кои носат параметри како IP адреса, мрежна маска, gateway, DNS сервери и други конфигурации. Доколку овие пакети бидат изменети или неправилно обработени, може да се добијат неточни мрежни параметри, што доведува до проблеми во комуникацијата на клиентските уреди.

Манипулацијата со пакетите може да се јави како резултат на конфигурациски грешки, технички дефекти или несинхронизирани уреди. Понекогаш е резултат и на софтверски проблеми или неправилно поставени DHCP параметри. Последицата е некоректно доделување на IP адреси, погрешни gateway или DNS информации и, генерално, нарушување на нормалното функционирање на мрежата.

Можности за решение:

1. Корекција на DHCP конфигурацијата
2. Проверка на легитимноста на DHCP серверите
3. Обнова на DHCP lease на клиентите
4. Привремено користење статички IP адреси
5. Мониторинг и анализа на DHCP логови

Со овие мерки се обезбедува стабилна и правилно конфигурирана мрежна околина, при што DHCP процесот функционира непречено и клиентските уреди добиваат точни мрежни параметри.

6.3. Broadcast ранливост

Broadcast ранливост се однесува на потенцијалните проблеми и ризици кои произлегуваат од користењето на broadcast комуникација во мрежата. Во компјутерските мрежи, broadcast е механизам со кој еден уред испраќа пакет кој се пренесува до сите уреди во истата локална мрежа (LAN). Иако broadcast е корисен за услуги како DHCP, ARP (Address Resolution Protocol) и други мрежни протоколи, тој може да создаде ранливости доколку не се контролира правилно.

Broadcast пакетите можат да бидат искористени за собирање информации за мрежата, идентификување на активни уреди, мапирање на IP и MAC адреси и анализа на

мрежниот сообраќај. Поради тоа, голем број на broadcast пакети или неправилно обработени broadcast пораки може да предизвикаат:

1. Пренатрупаност на мрежата (Network congestion) – голем број на broadcast пакети ја користи истата мрежна пропусност и може да ја намали ефикасноста на комуникацијата.
2. Повисока изложеност на информации – секој уред во мрежата го прима broadcast пакетот, што го прави подложен на потенцијални несакани анализи на податоците.
3. Можни системски дефекти – уредите кои постојано обработуваат голем број на broadcast пакети можат да бидат оптоварени или да доживеат намалена функционалност.

За да се намалат ризиците од broadcast ранливост, се применуваат техники како:

- Ограничување на broadcast доменот преку VLAN-ови и сегментација на мрежата.
- Филтрирање на broadcast пакети на ниво на комутатор или рутер за контролирање на непотребниот сообраќај.
- Следење и анализирање на broadcast сообраќајот за откривање на аномалии или неправилности.

Со правилна контрола и оптимизација на broadcast комуникацијата, можноста за ранливост се намалува, а мрежата останува стабилна и сигурна за сите уреди.

6.4. Ранливост на ниво 2

Layer 2 (Data Link Layer) во OSI моделот е слојот кој е одговорен за пренос на рамки (frames) преку физичката мрежна инфраструктура, идентификација на уредите преку MAC адреси и контрола на пристапот до медиумот. Иако овој слој е основа за функционирањето на мрежата, тој содржи повеќе вградени слабости поради начинот на кој е дизајниран и ниското ниво на безбедност во стандардните протоколи.

Ранливостите на Layer 2 произлегуваат од фактот дека овој слој главно работи со нешифирани податоци, користи broadcast комуникација и се потпира на доверба меѓу уредите. Како резултат, рамките што циркулираат во мрежата можат да бидат пресретнати, препратени, изменети или погрешно обработени доколку нема соодветна заштита. Нискиот слој не врши автентикација на уредите, што овозможува социјално или техничко „претставување“ на друг мрежен уред.

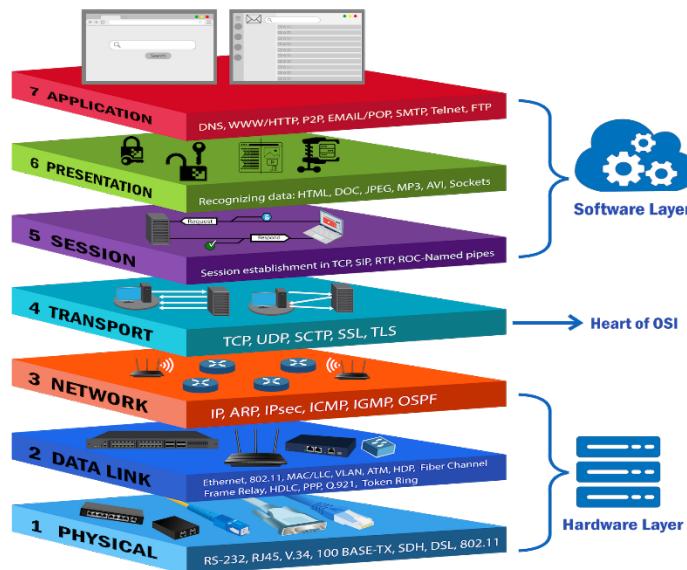
Некои примери на ранливости што произлегуваат од Layer 2 дизајнот, без да навлегуваме во конкретни напади, вклучуваат:

1. Несигурност на MAC адресите – MAC адресите лесно се менуваат, со што се нарушува нормалната работа на комутаторите.

2. Broadcast зависност – голем дел од комуникацијата на Layer 2 се изведува преку broadcast, што ги изложува сите уреди на примање и обработка на тие рамки.
3. Недостаток на контрола на пристап – комутаторите по дифолт ги прифаќаат сите рамки и не проверуваат дали доаѓаат од дозволени уреди.
4. Попречување на рамки (frame manipulation) – можно е да се изменат или реплицираат рамки, што може да доведе до погрешно функционирање на мрежата.
5. Недостаток на шифрирање – податоците што кружат во LAN најчесто се нешифрирани, што ја олеснува нивната анализа или злоупотреба.

Со оглед на тоа што Layer 2 претставува основа за комуникацијата во LAN околината, овие ранливиosti можат да доведат до нарушување на стабилноста на мрежата, погрешна распределба на сообраќајот или губење на податоци.

За да се намали влијанието на Layer 2 ранливиостите, се применуваат мерки како сегментација на мрежата, филтрирање на MAC адреси, користење управувани комутатори со безбедносни функции и надгледување на мрежниот сообраќај. Овие мерки помагаат да се задржи доверливоста и интегритетот на мрежната инфраструктура и да се спречат несакани однесувања на овој фундаментален слој.



Слика 10. OSI модел

7. DHCP напади

Благодарение на DHCP, администраторите не мораат рачно да конфигурираат мрежни поставки за секој уред, што го прави мрежниот менаџмент побрз и поефикасен. Сепак, токму поради својата улога во автоматската конфигурација, DHCP претставува и потенцијална точка на ранливост.

DHCP нападите се активности кои се насочени кон злоупотреба на DHCP протоколот за оневозможување на нормалната мрежна функционалност или за присвојување на мрежните ресурси. Овие напади можат да резултираат со неправилно дodelување IP адреси, прекинување на комуникацијата помеѓу клиентите и серверот, или пренасочување на сообраќајот преку злоупотребени уреди. Нападите најчесто се реализираат преку злоупотреба на DHCP пакетите, но нивната ефективност зависи и од начинот на конфигурација на мрежата, како и од мерките за заштита што се воведени.

Разбирањето на DHCP нападите е важно за обезбедување на стабилна и сигурна мрежна инфраструктура. Преку анализа на ранливостите на протоколот и можностите за заштита, администраторите можат да ги минимизираат ризиците и да го задржат континуираното функционирање на мрежата.

7.1. DHCP напади со гладување (Starvation)

Нападот со DHCP гладување може да резултира со напад со одбивање на услуги (DoS) или напад со човек во средина (MITM). За да го изврши овој напад, напаѓачот испраќа многу лажни DHCP Discover пораки со лажни изворни MAC адреси. DHCP серверот се обидува да одговори на сите овие лажни пораки и како резултат на тоа, базенот на IP адреси што ги користи DHCP серверот е исцрпан. Оттука, вистинскиот корисник нема да може да добие IP адреса преку DHCP. Ова резултира со DoS напад. Понатаму, напаѓачот може да постави лажен DHCP сервер за да додели IP адреси на легитимни корисници. Овој лажен сервер може да им обезбеди и гејтвеј рутер и DNS сервер на корисниците. Сега, целиот мрежен сообраќај може да се насочи преку машината на напаѓачот, а ова не е ништо друго освен MITM напад.



Слика 11. Напад со гладување

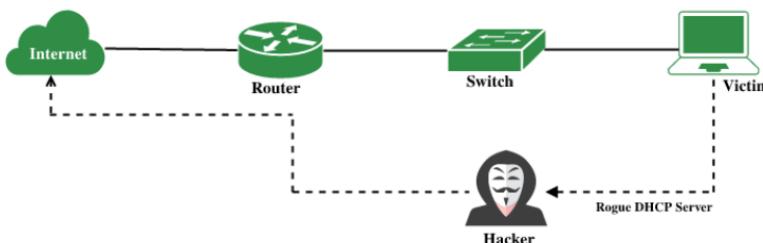
Од слика 5 IP адресата на DHCP серверот е 10.10.10.1/24 со подмрежна маска од 255.255.255.0. Значи, DHCP серверот може да додели 254 уникатни IP адреси. Сепак,

некои IP адреси се резервирали за статичко рутирање, па затоа може да бидат помалку од 254. Напаѓачот испраќа N DHCP Discover пакети, каде што N е многу голем во споредба со 254. Оттука, DHCP серверот повеќе не може да додели IP адреси. Нападот со DHCP гладување може да се спречи со имплементирање на безбедност на портата. Безбедноста на портот може да се конфигурира во прекинувач. Со безбедност на портата, можете да го ограничите бројот на MAC адреси што ги учи. Оттука, прекинувачот ќе ги препраќа пакетите со познати [MAC адреси](#), а другите ќе ги отфрла. На овој начин ќе спречи лажни пакети да стигнат до DHCP серверот.

7.2. Напади со нечесен DHCP сервер

Нападите на лажни DHCP сервери добиваат на популарност, но можат да се ублажат. Хакерот поставува лажен DHCP сервер и создава конфликт на IP адреси со еmitување на дупликат IP адреса. Хакерите се инфильтрираат во мрежа со напаѓање на безжичниот рутер, што го прават со ARP труење со цел да инјектираат лажни пакети во потокот на податоци што ги обработува рутерот. Овој генијален чекор им дава на хакерите континуиран пристап до мрежите преку прокси сервери и спам-пораки, што им отежнува на ИТ професионалците да спречат или дури и да детектираат сајбер напад. Потоа хакерот слуша за дојдовни врски и селективно одговара со злонамерни пораки како што се лажни барања за автентификација или вируси што предизвикуваат хаос на уредите на наивни корисници. Хакерот поставува лажен DHCP сервер и создава конфликт на [IP адреси](#) со еmitување на дупликат IP адреса.

Откако целосно хакерот ќе се инфильтрира во мрежата и ќе се постигне да се постави во позицијата, може да направи речиси сè што сака, почнувајќи од кражба на информации до инсталирање на злонамерен софтвер на вашиот компјутер со цел да го контролира од далечина.



Слика 12. Нечесен напад

Превенцијата од манипулација со DHCP е критична за одржување на безбедноста и функционалноста на една компјутерска мрежа. Најпрво, корисниците и администраторите треба да се поврзуваат само на доверливи безжични мрежи, бидејќи отворените или значително го зголемуваат ризикот од злонамерни DHCP сервиси и MITM напади.

Одржувањето на мрежната опрема со ажурирани фирмвери и безбедносни механизми овозможува брзо затворање на познати ранливости и спречува злоупотреби. Понатаму, администраторите треба активно да ги следат логовите на DHCP серверите

и мрежниот сообраќај со цел навремено откривање на сомнителни DHCP одговори или неовообичаено голем број барања.

За подобра заштита, важно е мрежата да биде конфигурирана така што само одредени уреди смеат да комуницираат со DHCP серверот, што ја намалува можноста неовластени клиенти да внесуваат лажни DHCP пораки. Дополнително, треба да се избегнува оставање на вклучено споделување датотеки преку рутери и мостови, бидејќи тоа создава дополнителни точки на напад. На корисничките уреди и на мрежната опрема мора да се постават сложени и неовообичаени лозинки, особено на администраторските профили, со цел спречување пристап од нападјачи кои ги користат стандардните фабрички лозинки.

Конечно, употребата на безбеден NAT (Network Address Translation) ја зголемува изолацијата помеѓу внатрешната мрежа и надворешните ресурси, што го отежнува директниот пристап до критичните системи во случај на DHCP манипулација. Со правилна комбинација од технички мерки, надзор и безбедносни практики, значително се намалуваат шансите за успешна злоупотреба на DHCP протоколот.

Важно хакерот прво ќе употреби напад врз безжичниот рутер со лажирање на MAC адреса и ARP труење. Потоа хакерот ќе се обиде да ги поврзе компјутерите со нечесниот уред наместо со рутерот. Откако тоа ќе се постигне, хакерот може да направи речиси сè, почнувајќи од кражба на информации до инсталирање на злонамерен софтвер на вашиот компјутер со цел да го контролира од далечина. Ова може да вклучува:

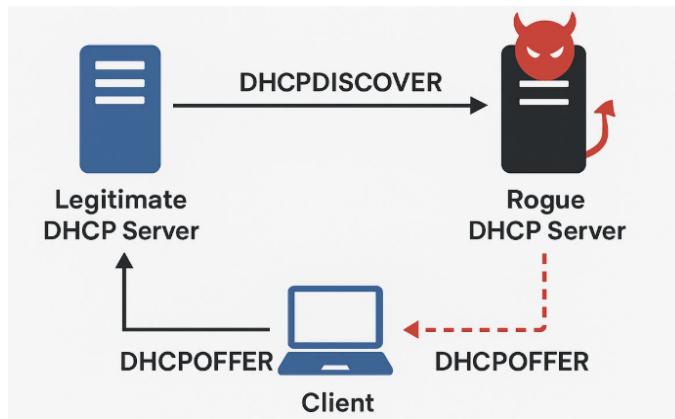
Крадење податоци, Преземање/Поставување вируси, Шпионски софтвер, Хакирање на вашиот компјутер, Спроведување напади од типот „човек во средината“ против вас. Хакерите користат лажни веб-страници (честопати фишинг) за да ги натераат корисниците нелегално да се најават на нивните сметки со нивните броеви на социјално осигурување и лозинки.

7.3. DHCP лажирање (Spoofing)

DHCP лажирањето претставува сериозен безбедносен напад во компјутерските мрежи и се заснова на поставување лажен DHCP сервер кој им одговара на клиентите побрзо од легитимниот сервер, со што им доделува злонамерни или неточни мрежни конфигурации. Овој тип на напад го искористува фактот што DHCP протоколот нема вградена автентификација, па клиентот ја прифаќа првата DHCP понуда што ќе ја добие, без да може да утврди дали потекнува од доверлив извор. На тој начин, напаѓачот може да го пренасочи мрежниот сообраќај преку своја машина, поставувајќи се како стандарден портал или DNS сервер, што овозможува пресретнување, следење и манипулација на податоците што циркулираат во мрежата.

Функционирањето на DHCP лажирањето се базира на пресретнување на почетните DHCP пораки. Кога клиентот испраќа DHCPDISCOVER за да пронајде DHCP сервер, нелегитимниот сервер поставен од напаѓачот брзо одговара со DHCPOFFER во кој внесува параметри под негова контрола. Така, уредот добива погрешен default

gateway, манипулирани DNS записи или друга мрежна конфигурација што овозможува напаѓачот да се постави во позиција на „човек-во-средина“. Во некои случаи, напаѓачот претходно спроведува DHCP Starvation напад, испраќајќи голем број DHCPPREQUEST пораки со лажни MAC адреси, со што го исцрпува базенот на IP адреси на легитимниот сервер и го прави неспособен да услужи нови клиенти. Со исцрпен DHCP пул, злонамерниот сервер станува единствениот што може да одговара на новите барања и така ја презема контролата врз мрежата. Во пракса, DHCP лажирањето често се јавува во комбинација со напади како Man-in-the-Middle, каде што напаѓачот не само што го контролира насочувањето на сообраќајот, туку и активно ги пресретнува чувствителните податоци, краде акредитиви или пренасочува кон лажни веб-страници. Напаѓачите можат да соберат NetNTLM хешови преку присилна автентификација, да го прекинат пристапот до мрежата преку исцрпување на IP пулот или да го пренасочат целиот сообраќај за анализирање и манипулирање. Овие сценарија јасно укажуваат на тоа дека DHCP лажирањето носи ризици како пресретнување на податоци, неовластен пристап, целосни мрежни прекини, кражба на акредитиви и можност за дополнителни напади по преземањето на контролата врз сообраќајот.



Слика 13. Лажен напад

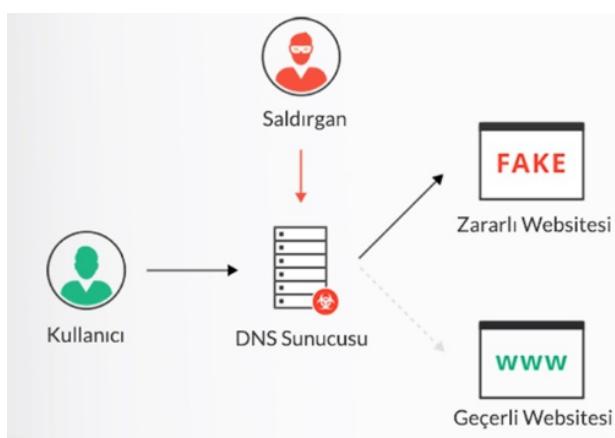
Заштитата од вакви напади бара комбинација од повеќе безбедносни механизми во самата инфраструктура. DHCP Snooping е една од најважните мерки, бидејќи го ограничува испраќањето на DHCP понуди само на доверливи порти и автоматски ги блокира лажните сервери. Port Security дополнително го ограничува бројот на MAC адреси на една порта и ги спречува неовластените уреди да се поврзат на мрежата. VLAN сегментацијата овозможува DHCP сообраќајот да биде изолиран во одделни мрежни сегменти, со што се намалува површината за напад. IP Source Guard филтрира сообраќај според IP-MAC врзувања и спречува лажирање на IP адреси. Како дополнителна мерка, редовните пенетрациони тестови овозможуваат навремено откривање на ранливостите во мрежната инфраструктура и подобрување на безбедносните политики.

Како целина, DHCP лажирањето е сериозна закана која го нарушува интегритетот и сигурноста на мрежата преку манипулирање со основните мрежни параметри. Со оглед на природната ранливост на DHCP протоколот, неопходно е организациите да применуваат повеќеслојна заштита и внимателно да го следат мрежниот сообраќај за да спречат нечисти понуди и да ја одржат стабилноста и безбедноста на системите.

7.4. DNS киднапирање

DNS киднапирањето претставува техника со која напаѓачите неовластено ги менуваат DNS поставките со цел да ги пренасочат корисниците кон лажни или малициозни веб-страници. Овој напад е опасен затоа што корисникот не забележува дека е пренасочен, бидејќи процесот на преведување на доменските имиња во IP адреси секогаш се одвива во позадина. DNS функционира како „именик на интернетот“ – кога корисник внесува домен, DNS го претвора во IP адреса за да се отвори вистинската страница. Затоа, секој обид за негово манипулирање директно го нарушува целокупниот пристап до интернет ресурсите.

Нападите најчесто се изведуваат со инсталирање малициозен софтвер на уредот на корисникот или со компромитирање на DNS комуникацијата. На пример, напаѓач може



Слика 14. DNS киднапирање

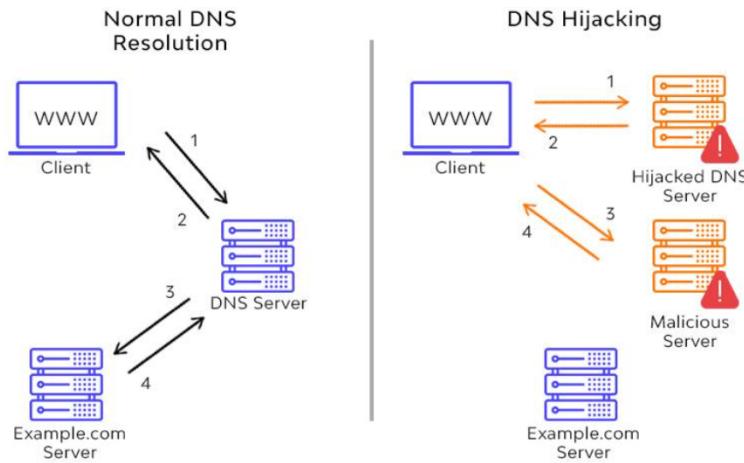
да постави лажен DNS сервер кој ќе одговара со изменети записи и ќе го упатува корисникот кон измамнички страници. Таквите страници често служат за фишинг, крадење лозинки, банкарски податоци или прикажување реклами со финансиска корист за напаѓачот. Дополнително, нападот може да влијае врз угледот и довербата на организациите, бидејќи корисниците може да мислат дека нивните услуги не функционираат или дека се небезбедни.

DNS хиџекингот може да се појави на неколку начини: преку промена на DNS поставки на компјутерот на жртвата, преку злоупотреба на ранлив рутер, преку пресретнување на комуникацијата меѓу корисникот и DNS серверот или преку директно пробивање на DNS серверот и измена на неговите записи.

За намалување на ризикот, организациите и корисниците треба да применуваат повеќе мерки. На серверско ниво, корисно е ограничување на пристапот до DNS поставките, користење заштитни сидови, редовно ажурирање, избегнување на истовремено користење на резолвер и авторитативен сервер на ист систем и спречување неовластени преноси на DNS зони. Дополнителна заштита овозможува DNSSEC, кој користи дигитални потписи за да потврди дека DNS одговорите се автентични.

Кај корисниците, препорачливо е редовно менување на лозинките за рутерите, користење антивирус, избегнување сомнителни мрежи и употреба на VPN кога е потребно. Ако интернет провајдерот користи сопствено пренасочување, можно е да се користи алтернативен DNS сервис што го блокира тоа однесување.

Иако DNS хијекингот е чест и со текот на времето се појавуваат нови методи на напад, навремената превенција и редовниот надзор врз инфраструктурата значително ја намалуваат веројатноста за компромитирање. Затоа, и организациите и индивидуалните корисници треба да одржуваат соодветно ниво на безбедност и постојано да ги следат своите DNS поставки за да избегнат нарушување на приватноста и функционирањето на интернет услугите.



Слика 15. Споредба помеѓу DNS со зачувана резолуција и киндапиран сервер

7.5. Пренасочување на портал

Gateway редирекцијата во DHCP претставува состојба кога клиентот преку DHCP добива погрешна или манипулирана default gateway адреса. Наместо валидната IP адреса на рутерот, клиентот може да добие адреса на уред што не е вистински gateway, што се случува поради погрешна конфигурација или намерна манипулација на DHCP пораките. Кога клиентот ќе ја прифати оваа погрешна gateway информација, целиот негов мрежен сообраќај се пренасочува кон неавторизиран уред, што може да резултира со губење на интернет конекција, блокирање на сообраќај или негово пресретнување и анализирање. Бидејќи gateway е клучна точка за рутирање кон надворешни мрежи, секоја несоодветна промена директно го нарушува функционирањето на мрежата. За да се спречат вакви ситуации, се применуваат механизми како DHCP Snooping, ограничување на доверливи DHCP извори, статичка конфигурација за критични уреди и континуиран мониторинг за неочекувани DHCP Offers или ACK пораки.

7.6. Заробување на сообраќајот

Traffic capture претставува напреден процес на пресретнување и снимање на мрежниот сообраќај што се пренесува низ одредена мрежа, интерфејс или уред. Неговата главна цел е да се овозможи увид во тоа кои пакети се движат, од каде потекнуваат, каде одат и што точно носат во себе. Со снимање на сообраќајот,

администраторите и безбедносните аналитичари добиваат можност да го разгледаат секој пакет поединечно – од најниско ниво (Ethernet frame), преку IP и TCP/UDP заглавија, па сè до апликативниот слој. Ова овозможува откривање неисправни конфигурации, мрежни грешки, доцнења, загуби на пакети, но и понапредни ситуации како сомнителни активности, неовластени комуникации, малициозни пакети или аномалии во однесувањето на мрежата.

Traffic capture се користи во повеќе сценарија: при траблшутинг за да се види зошто некој сервис не функционира, при оптимизација на перформанси за да се идентификуваат тесни грла, во безбедност за откривање скриени конекции и нападни обиди, како и во форензика за реконструкција на настани по инцидент. Алатки како Wireshark, tcpdump, tshark и NetworkMiner овозможуваат визуелизација на пакетите, филтрирање на специфични комуникации, репродукција на TCP сесии и следење на протоколи во живо. Овие алатки всушност го „разголуваат“ сообраќајот и дозволуваат да се види секој бит што се пренесува преку мрежата.

Особено интересен аспект е тоа што traffic capture може да открие дури и проблеми кои корисникот воопшто не ги забележува – како ARP конфликти, DNS неправилности, повторени пакети, па дури и индикации за MitM активности. Од друга страна, бидејќи во сообраќајот честопати се пренесуваат чувствителни податоци, снимањето мора да се врши внимателно и со дозвола, затоа што неправилно користење може да резултира со нарушување на приватноста.

Во суштина, traffic capture претставува прозорец кон целокупната мрежна комуникација – алатка која ја прави „невидливата“ мрежна активност видлива и разбиралива, овозможувајќи прецизна анализа, откривање проблеми и засилување на безбедноста.

8. Техника за заштита на DHCP

Dynamic Host Configuration Protocol (DHCP) претставува еден од клучните сервиси во секоја модерна мрежа, бидејќи автоматски доделува IP адреси, мрежни параметри и други конфигурации на уредите што се приклучуваат. Неговата леснотија на работа и автоматизацијата го прават неопходен за домашни, корпоративни и облачни системи. Но, токму таа отвореност и доверба меѓу клиентите и серверот ја прават DHCP инфраструктурата ранлива. Бидејќи протоколот по своја природа не користи автентикација и не проверува дали уредот навистина е легитимен, можни се разни манипулации со DHCP пакетите, појава на лажни сервери, преплавување со барања и погрешно насочување на мрежниот сообраќај.

Од тие причини, развиени се различни техники за заштита на DHCP, чија цел е да спречат неовластени уреди да добијат мрежни ресурси, да блокираат лажни DHCP одговори и да овозможат контрола и следење на целокупниот процес на доделување IP адреси. Овие техники не само што ја зголемуваат безбедноста, туку обезбедуваат стабилност и предвидливост на мрежата – што е особено важно во големи системи како кампуси, компании и дата-центри. Следниот дел ќе ги обработи најзначајните методи за заштита: од основни мрежни ограничувања до напредни функции како DHCP Snooping, порт-безбедност, автентикација и мониторинг. Целта е да се добие јасна слика како мрежниот инженер може да изгради сигурно DHCP опкружување и да минимизира ризиците од злоупотреба.

8.1. NETWORK ACCESS CONTROL (IEEE 802.1X)

Процесот започнува во моментот кога крајниот уред, познат како *suplicant*, се поврзува на жичена или безжична мрежа. Во оваа почетна фаза, мрежниот уред кој ја контролира комуникацијата, наречен *authenticator* (најчесто *switch* или *wireless access point*), ја задржува својата порта во неовластена состојба. Во таква состојба, целиот IP сообраќај, вклучувајќи ги и DHCP пакетите, е блокиран. Единствениот дозволен тип на комуникација се EAP (Extensible Authentication Protocol) пораки, кои се користат исклучиво за автентикација и се пренесуваат преку протоколот EAP over LAN (EAPoL).

Supplicant-от иницира автентикациски процес со испраќање EAPoL-Start порака, по што authenticator-от го проследува автентикациското барање до централниот сервер за автентикација, најчесто RADIUS сервер. RADIUS серверот ја анализира автентикациската информација врз основа на конфигурираните политики и методи на автентикација, како што се корисничко име и лозинка, дигитални сертификати или машинска автентикација. Во текот на овој процес, крајниот уред сè уште нема IP адреса и нема можност за пристап до мрежни ресурси, што значително ја намалува површината за потенцијални напади.

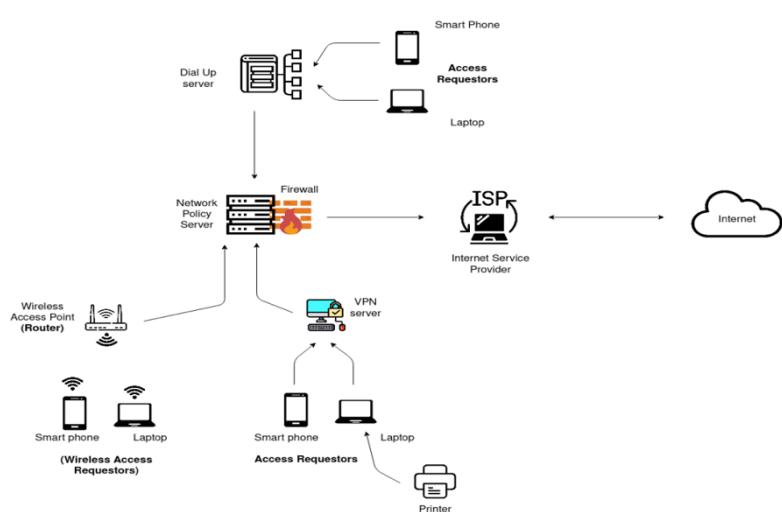
Доколку автентикацијата биде успешна, RADIUS серверот испраќа позитивен одговор до authenticator-от, кој ја менува состојбата на портата од неовластена во овластена. Само во овој момент се овозможува нормален мрежен сообраќај, вклучувајќи ги и DHCP пораките. Клиентот тогаш иницира DHCP процес со испраќање DHCP Discover порака, со што започнува постапката за динамичко доделување на IP адреса. Овој редослед е клучен за безбедноста, бидејќи спречува неавтентицирани уреди да добијат валидна IP адреса и да учествуваат во мрежната комуникација.

Интеграцијата помеѓу 802.1X и DHCP серверот овозможува напредна контрола на мрежниот пристап преку динамично доделување на мрежни параметри врз основа на идентитетот на корисникот или уредот. RADIUS серверот, покрај информацијата за успешна автентикација, може да испрати дополнителни атрибути како што се VLAN идентификатор, политики за пристап или ограничувања на сообраќајот. Врз основа на овие атрибути, authenticator-от може да го смести клиентот во соодветна VLAN, од која DHCP серверот доделува IP адреса од специфичен IP опсег. На овој начин, различни категории на корисници – вработени, гости или администратори – можат да добијат различни нивоа на мрежен пристап, иако се поврзуваат преку иста физичка инфраструктура.

Овој модел овозможува и имплементација на карантински или рестриктивни мрежи, каде што уреди кои не ги исполнуваат безбедносните политики добиваат ограничена IP конфигурација и пристап само до одредени сервиси, како што се системи за ажурирање или портали за регистрација. Така, DHCP серверот станува активен дел од безбедносната архитектура, а не само сервис за автоматска конфигурација на мрежни параметри.

Комбинираната употреба на 802.1X и DHCP значително ја намалува можноста за злоупотреби како што се неовластен пристап, DHCP лажирање и IP конфликти, бидејќи само автентицирани уреди можат да добијат валидна IP адреса и да учествуваат во мрежата. Дополнително, овој пристап обезбедува подобра видливост и контрола врз уредите во мрежата, централизирано управување со политиките за пристап и зголемено ниво на доверливост и интегритет на мрежната комуникација. Како резултат на тоа, Network Access Control базиран на 802.1X претставува клучен елемент во современите безбедносни мрежни архитектури, особено во средини со високи безбедносни барања и голем број на динамички корисници и уреди.

Дијаграмот за Network Access Control (NAC) ја прикажува мрежната архитектура на една софтверска компанија и ги илустрира механизмите што се користат за заштита на приватната мрежа од неовластен пристап. Основната цел на NAC е да овозможи дека само автентицирани, овластени и со политики усогласени корисници и уреди можат да пристапат до мрежните ресурси. Со напредокот на технологијата и примената на



Слика 16. Процес на мрежен пристап

современи мрежни стратегии, ограничувањата за некорпоративни и непроверени уреди стануваат сè построги, со што значително се зголемува безбедноста на целокупната мрежна инфраструктура. Network Access Control претставува клучен безбедносен механизам кој го ограничува пристапот исклучиво на доверливи уреди што ги исполнуваат дефинираните безбедносни политики.

Во прикажаната мрежна структура се користат три различни типови рутери. Првиот е dial-up интернет рутер, кој овозможува поврзување преку обична телефонска линија и пристап преку однапред дефиниран сет на телефонски броеви. Иако оваа технологија денес е речиси напуштена и не се користи за редовна корпоративна комуникација, софтверската компанија ја задржува само за основен интернет пристап или поради потреби за компатибилност со постари системи.

Покрај тоа, компанијата користи безжична пристапна точка (Wireless Access Point), која денес е еден од најзастапените начини за мрежно поврзување. Безжичната комуникација овозможува голем број уреди, како лаптопи, мобилни телефони и таблети, да се поврзат на интернет без употреба на кабли. Комуникацијата помеѓу безжичниот рутер и уредите се одвива преку радио сигнали кои се испраќаат и примаат во двета правци. Дополнително, повеќето безжични рутери поддржуваат и жично поврзување преку Ethernet кабел и најчесто располагаат со до четири физички порти.

Третиот тип на поврзување во софтверската компанија е преку Virtual Private Network (VPN). Компанијата поседува сопствен VPN сервер, кој овозможува создавање на криптиран тунел преку кој корисниците можат безбедно да пристапат до внатрешните мрежни ресурси и интернет услугите. VPN технологијата обезбедува доверливост, интегритет и заштита на податоците, особено при далечински пристап. Дополнително, VPN овозможува прикривање на IP адресата, при што вистинската IP адреса на корисникот се заменува со друга адреса, што придонесува за зголемена приватност и можност за пристап до регионално ограничени веб-страници. Иако првично VPN технологијата била развиена за поддршка на работа од далечина, нејзината примена денес е значително проширена и во личниот и во професионалниот контекст.

Покрај трите рутери, мрежната архитектура вклучува и сервер за мрежни политики (Network Policy Server), кој претставува централен елемент за управување со

автентификацијата, авторизацијата и распределбата на ресурсите во мрежата. Овој сервер дефинира и спроведува безбедносни политики што го регулираат нивото на пристап на корисниците до различни мрежни ресурси. Политиките се креираат од страна на мрежниот администратор во согласност со организациските потреби и работните тимови, со цел да се обезбеди ефикасност и сигурност. Една од најзначајните предности на серверот за политики е заштитата на приватноста на корисниците и контролата врз пристапот до чувствителни податоци.

Меѓу најважните политики што се применуваат при пристап до интернет се задолжителната употреба на HTTPS протоколот, кој овозможува безбедна и криптирана комуникација помеѓу клиентот и интернет сервисите. Дополнително, енкрипцијата на Voice over Internet Protocol (VoIP) комуникацијата се управува на транспортниот слој, што претставува уште една задача на серверот за политики. Исто така, се применува и IP whitelisting, механизам со кој пристапот до мрежата се ограничува само на претходно одобрени и доверливи уреди. Ова е особено важно кај безжичните мрежи, каде што потенцијално може да се обидат да се поврзат голем број неовластени уреди.

Firewall-от претставува стандардна и неопходна компонента во безбедносната мрежна инфраструктура. Тој функционира како заштитна бариера помеѓу доверливата внатрешна мрежа и недоверливите надворешни мрежи, како што е интернетот. Со примена на однапред дефинирани безбедносни правила, firewall-от го следи, филтрира и контролира влезниот и излезниот сообраќај, спречувајќи неовластен пристап и потенцијални безбедносни закани.

Откако податоците ќе поминат низ firewall-от и механизмите за контрола на политики, тие се проследуваат до интернет сервис провајдерот (ISP) во криптирана и безбедна форма. ISP потоа ги насочува барањата кон соодветните DNS сервери и ги презема потребните податоци од интернет, по што одговорите се враќаат назад кон мрежата на софтверската компанија. Овој контролиран и структуриран тек на податоци овозможува сигурна и усогласена комуникација помеѓу внатрешните хостови и надворешните интернет сервиси.

Без примена на такви одбранбени механизми, корпоративните мрежи би биле исклучително ранливи на чести безбедносни напади. Network Access Control овозможува ефикасна и проактивна безбедносна стратегија преку осигурување дека сите уреди поврзани на мрежата се во согласност со дефинираните политики. Како заклучок, интеграцијата на NAC, сервери за мрежни политики, firewall и VPN технологија претставува основа за безбедна, контролирана и ефикасна комуникација помеѓу корисниците и интернетот во современа софтверска компанија.

8.2. DHCP Шпионирање (Snooping)

DHCP Snooping претставува безбедносен механизам на вториот слој од OSI моделот, чија основна намена е заштита на мрежата од неовластени уреди што се обидуваат да се претстават како DHCP сервери. Овој механизам функционира преку

активно следење и филтрирање на DHCP сообраќајот што поминува низ switch-от, со што се блокираат одредени типови DHCP пораки од недоверливи порти и се ограничува бројот на DHCP барања по уред. Главната цел на DHCP Snooping е спречување на DHCP spoofing напади, кои можат да доведат до сериозни нарушувања на безбедноста и доверливоста на мрежната комуникација.

За да се разбере значењето на DHCP Snooping, најпрво е потребно да се разгледа основниот начин на работа на DHCP протоколот. Кога еден уред се поврзува на мрежа, тој започнува повеќечекорен процес за добивање IP адреса. Уредот најпрво испраќа DHCP Discover порака, со која сигнализира дека бара IP адреса. DHCP серверот одговара со DHCP Offer порака, во која нуди слободна IP адреса, по што клиентот испраќа DHCP Request како потврда дека ја прифаќа понудата. Процесот завршува со DHCP ACK порака од серверот, со која официјално се доделува IP адресата. Важно е да се нагласи дека оваа комуникација по дифолт не е автентицирана, што претставува сериозна безбедносна слабост.

Поради отсъството на автентикација, постои можност злонамерен уред во истата мрежа да се претстави како DHCP сервер и да испраќа лажни DHCP Offer и DHCP ACK пораки. Во такво сценарио, клиентските уреди може да прифатат погрешни мрежни параметри, како IP адреса, default gateway или DNS сервер, што му овозможува на напаѓачот да го пресретнува и анализира целиот сообраќај (man-in-the-middle напад). Дополнително, напаѓачите можат да извршат и DHCP starvation напад, при што испраќаат голем број DHCP барања за да ги исцрпат сите достапни IP адреси, со што легитимните клиенти остануваат без мрежен пристап, а напаѓачот може да се наметне како единствен DHCP сервер.

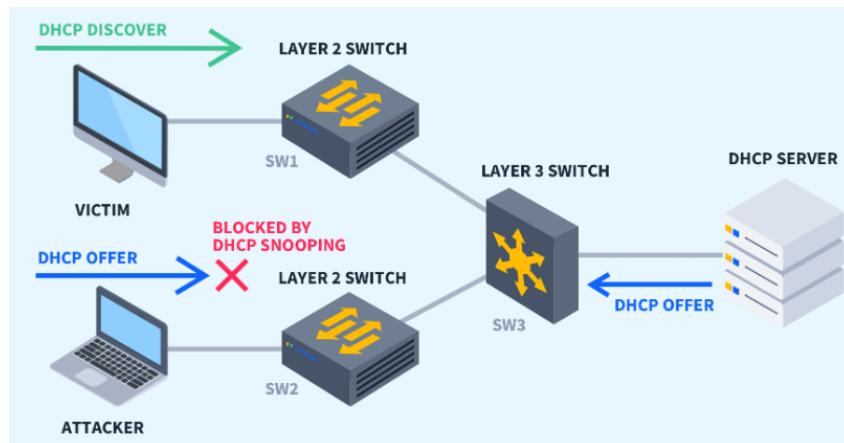
DHCP Snooping е воведен токму како одговор на овие закани. Тој овозможува администраторите на мрежата да ги дефинираат портите на switch-от како доверливи (trusted) и недоверливи (untrusted). Само доверливите порти, кои обично водат кон легитимен DHCP сервер или кон uplink кон друг мрежен уред, имаат дозвола да пренесуваат DHCP Offer и DHCP ACK пораки. Сите останати порти, најчесто оние на кои се поврзани крајни корисници, се сметаат за недоверливи и преку нив е дозволено само испраќање на клиентски DHCP пораки, како DHCP Discover и DHCP Request. Доколку од недоверлива порта се детектира DHCP серверска порака, switch-от автоматски ја блокира.

Покрај филтрирањето на DHCP сообраќајот, DHCP Snooping овозможува и заштита од DHCP starvation напади преку механизам за ограничување на брзината (rate limiting). Со ограничување на бројот на DHCP пакети што можат да поминат низ недоверлива порта во одреден временски интервал, значително се намалува можноста напаѓач да испрати доволен број барања за да ги исцрпи IP ресурсите. Овој пристап обезбедува стабилност и достапност на DHCP услугата за легитимните корисници.

Дополнителна придобивка од DHCP Snooping е креирањето на DHCP Snooping binding tabela, во која се запишуваат податоци за секој клиент што добил IP адреса, вклучувајќи ја неговата MAC адреса, доделената IP адреса, VLAN идентifikаторот и

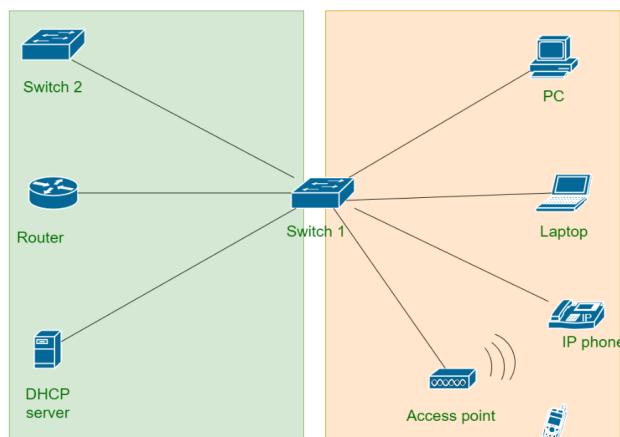
портата на switch-от. Оваа табела претставува основа за имплементација на други напредни безбедносни механизми, како Dynamic ARP Inspection и IP Source Guard, кои дополнително ја зајакнуваат заштитата на мрежата.

Во практична примена, DHCP Snooping мора внимателно да се конфигурира, бидејќи по дифолт сите порти се третираат како недоверливи. Доколку администраторот не ги означи правилно портите што водат до DHCP серверот како trusted, легитимниот DHCP сообраќај може да биде блокиран и уредите нема да добијат IP адреси. Затоа е неопходно редовно следење на логовите на switch-от и проверка на конфигурацијата. Дополнително, препорачливо е конфигурацијата на switch-от да се чува како резервна копија, за да се овозможи брзо враќање на системот во случај на грешка или инцидент.



Слика 17. Анализа на напад со шпионирање

Како заклучок, DHCP Snooping претставува едноставен, но исклучително ефикасен безбедносен механизам кој значително ја зголемува заштитата на мрежата од DHCP spoofing и DHCP starvation напади. Со комбинирање на контрола на портите, мониторинг на DHCP сообраќајот и ограничување на брзината на барањата, DHCP Snooping обезбедува дека ниту еден неовластен уред не може да се наметне како лажен DHCP сервер. Поради тоа, овој механизам се смета за основна и неопходна компонента во современите корпоративни мрежи и често претставува темел за имплементација на напредни безбедносни стратегии.



Слика 18. Споредба на порти преку ниво на доверба

8.3. Dynamic Arp Inspection – DAI

Dynamic ARP Inspection (DAI) претставува напреден безбедносен механизам на вториот слој од OSI моделот, чија основна цел е заштита на локалните мрежи од ARP poisoning и ARP spoofing напади. ARP (Address Resolution Protocol) е протокол кој се користи за мапирање на IP адреси со соодветни MAC адреси во локалната мрежа, овозможувајќи правилна испорака на Ethernet рамки. Меѓутоа, поради тоа што ARP протоколот по своја природа не вклучува механизми за автентикација, тој е подложен на злоупотреби, при што напаѓач може да испраќа лажни ARP пораки и да го наруши нормалното функционирање на мрежата. Dynamic ARP Inspection е дизајниран токму за да ја надмине оваа слабост преку активна проверка и филтрирање на ARP сообраќајот.

DAI функционира со анализирање на сите ARP пораки што минуваат низ switch-от и нивна споредба со претходно дефинирани или динамички креирани доверливи информации. Кога ќе биде детектирана ARP порака која содржи несоодветна или нелегитимна IP–MAC комбинација, switch-от ја отфрла пораката и на тој начин спречува погрешно ажурирање на ARP табелите кај крајните уреди. Овој механизам значително го намалува ризикот од man-in-the-middle напади, пренасочување на сообраќај и неовластен пристап до чувствителни податоци.

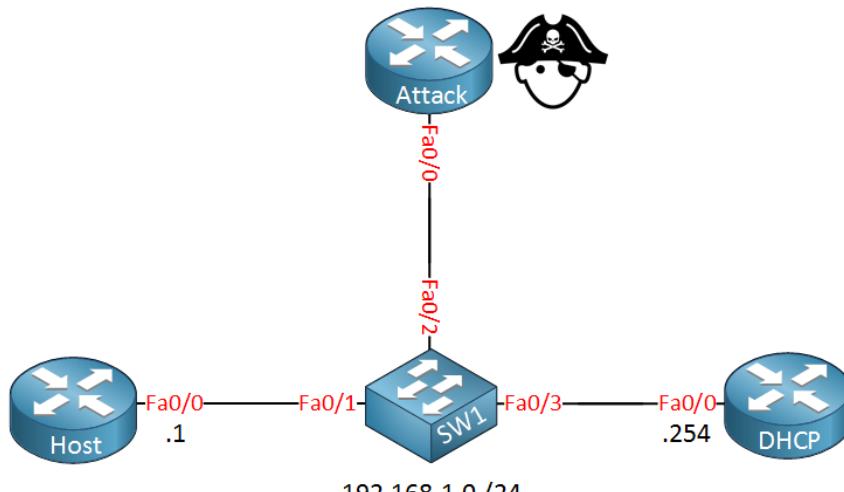
Клучен аспект во функционирањето на Dynamic ARP Inspection е неговата тесна поврзаност со DHCP Snooping. DHCP Snooping креира и одржува binding табела во која се чуваат валидни IP–MAC врски за уредите што легитимно добиле IP адреси од DHCP серверот. Оваа табела претставува доверлив извор на информации врз основа на кој DAI ја врши својата валидација. Кога DAI е активиран, switch-от ги споредува ARP пораките со записите од DHCP Snooping binding табелата и дозволува само оние ARP пораки што се усогласени со веќе познатите и доверливи IP–MAC парови.

Во сценарио без Dynamic ARP Inspection, напаѓач може лесно да испрати лажни ARP одговори, при што ќе тврди дека неговата MAC адреса одговара на IP адресата на рутерот или на друг уред во мрежата. Како резултат, сообраќајот од другите уреди се пренасочува кон напаѓачот, што овозможува прислушување, модификација или блокирање на податоците. Со активиран DAI, ваквите лажни ARP пораки се детектираат и блокираат, бидејќи нивните IP–MAC комбинации не се совпаѓаат со доверливите записи добиени од DHCP Snooping.

Дополнително, Dynamic ARP Inspection користи концепт на доверливи (trusted) и недоверливи (untrusted) порти, слично како DHCP Snooping. ARP сообраќајот што пристигнува преку доверливите порти, како што се оние поврзани со рутери или сервери, се смета за легитимен и не се подложува на детална проверка. Од друга страна, ARP пораките што доаѓаат преку недоверливите порти, каде што најчесто се поврзани крајните уреди, се строго инспектираат и валидираат. Оваа поделба овозможува ефикасна заштита без значително влијание врз перформансите на мрежата.

Табелите со доверливи IP→MAC врски претставуваат централна компонента на DAI. Тие може да бидат динамички генериирани преку DHCP Snooping или статички конфигурирани од страна на мрежниот администратор во случаи кога уредите користат статички IP адреси. Преку овие табели, switch-от добива јасна референтна точка за тоа кои ARP пораки се легитимни и кои претставуваат потенцијална закана. На овој начин, DAI не само што реагира на нападите, туку проактивно спречува нивна реализација.

Како заклучок, Dynamic ARP Inspection претставува суштински безбедносен механизам за заштита на локалните мрежи од ARP poisoning напади. Неговата интеграција со DHCP Snooping овозможува создавање на сигурна и доверлива основа за валидација на ARP сообраќајот, преку користење на точни и проверени IP-MAC врски. Со имплементација на DAI, организациите значително ја подобруваат безбедноста, стабилноста и доверливоста на својата мрежна инфраструктура, што го прави овој механизам неопходен дел од современите корпоративни мрежи.



Слика 19. Безбедност со DAI

Како илустративен пример за значењето на Dynamic ARP Inspection, може да се разгледа сценарио во кое злонамерен уред е поврзан на локалната мрежа на една организација. Напаѓачот испраќа лажни ARP одговори до останатите уреди во мрежата, тврдејќи дека неговата MAC адреса одговара на IP адресата на default gateway-от.

Поради тоа што ARP протоколот не користи автентификација, легитимните уреди ги прифаќаат овие пораки и го ажурираат својот ARP кеш со неточни IP-MAC информации. Како резултат, целиот мрежен сообраќај кој требало да биде испратен кон рутерот се пренасочува кон уредот на напаѓачот, што му овозможува да го прислушува, модифицира или блокира сообраќајот, односно да изврши man-in-the-middle напад.

Во мрежа каде што се имплементирани DHCP Snooping и Dynamic ARP Inspection, ваквото сценарио е ефикасно спречено. DHCP Snooping претходно има креирано binding табела со валидни IP-MAC врски за сите уреди што легитимно добиле IP адреса од DHCP серверот. Кога напаѓачот ќе се обиде да испрати лажна ARP порака, Dynamic ARP Inspection ја споредува IP-MAC комбинацијата од пораката со записите во DHCP Snooping табелата. Бидејќи MAC адресата на напаѓачот не одговара на легитимната MAC адреса поврзана со IP адресата на gateway-от, ARP пораката се смета за

нелегитимна и автоматски се блокира од страна на switch-от. На тој начин се спречува труење на ARP кешот кај останатите уреди и се зачувува интегритетот на мрежната комуникација.

Овој пример јасно ја прикажува практичната вредност на Dynamic ARP Inspection како проактивен механизам за заштита, кој не само што детектира, туку и директно спречува ARP poisoning напади. Во комбинација со DHCP Snooping, DAI овозможува високо ниво на доверливост и безбедност во локалните мрежи, што е од особена важност во корпоративни средини со голем број корисници и чувствителни податоци.

8.4. Заштита на IP извори

Современите корпоративни и институционални мрежи се соочуваат со големи безбедносни предизвици на Layer 2 ниво, особено во контекст на неовластен пристап, манипулација со IP и MAC адреси и ARP spoofing напади. За да се обезбеди интегритетот и доверливоста на локалната мрежа, администраторите користат комбинација од DHCP Snooping, Dynamic ARP Inspection (DAI) и IP Source Guard (IPSG). Овие технологии заедно формираат повеќеслојна безбедносна архитектура која спречува најчестите напади на мрежното ниво.

DHCP Snooping претставува првиот слој на одбрана против DHCP spoofing и неовластено IP доделување. Кога уред се поврзува на мрежата, тој испраќа DHCP Discover порака за да добие IP адреса, а DHCP серверот одговара со DHCP Offer. Клиентот ја прифаќа понудената адреса со DHCP Request, а серверот го финализира процесот со DHCP ACK.

Напаѓачот може да користи лажен DHCP сервер за да испраќа DHCP Offer пораки и да насочи сообраќај кон својот уред, овозможувајќи прислушување или IP hijacking. DHCP Snooping овозможува дефинирање на trusted порти, каде се поврзани DHCP сервери или други сигурни уреди, кои можат да испраќаат DHCP Offer и ACK пораки. Сите други порти се третираат како untrusted, и нивните DHCP пораки се верификуваат или блокираат. Дополнително, функцијата за rate limiting спречува DHCP starvation, каде напаѓач испраќа голем број барања за IP адреси со цел да ги исцрпи ресурсите на DHCP серверот. На овој начин, DHCP Snooping обезбедува доверлив извор на IP-MAC информации, кој е критичен за понатамошните безбедносни механизми.

Dynamic ARP Inspection (DAI) го следи и верификува ARP сообраќајот на мрежата за да спречи ARP poisoning. ARP протоколот, кој овозможува поврзување на IP адресите со физичките MAC адреси, е ранлив бидејќи не користи автентикација. Напаѓачи можат да испраќаат лажни ARP пораки и да се претстават како друг уред, најчесто default gateway, за да прислушуваат, модифицираат или прекинуваат сообраќај.

DAI користи доверливи IP-MAC комбинации од DHCP Snooping binding табелата за валидација. Секој ARP пакет што пристигнува од untrusted порти се проверува, а ако не се усогласува со доверливите записи, се блокира. При тоа, switch-от генерира логови или аларми, овозможувајќи навремено откривање на потенцијални напади.

Пример: Во корпоративна мрежа, напаѓач се обидува да испраќа ARP пораки кои тврдат дека неговата MAC адреса е поврзана со IP адресата на gateway-от. Со активиран DAI, лажните ARP пораки се веднаш блокирани и напаѓачот не може да прислушува или да манипулира со сообраќајот, обезбедувајќи сигурност и континуитет на комуникацијата.

IP Source Guard (IPSG) е дополнителен слој на заштита кој спречува IP spoofing преку контрола на изворниот сообраќај. Секој пакет кој пристигнува од untrusted порта се проверува според IP и MAC адресата и се споредува со DHCP Snooping binding табелата. Пакетите кои не се усогласуваат се блокираат, спречувајќи неовластен пристап.

Пример: Напаѓач испраќа пакети со IP адресата на легитимен уред. Без IPSG, мрежата би ги прифатила овие пакети, овозможувајќи прислушување или модификација на податоци. Со активиран IPSG, пакетите се веднаш блокираат, а администраторите добиваат известување за обидот за злоупотреба. Дополнително, rate limiting ја намалува можноста за злоупотреба на IP ресурси и дополнително ја зголемува сигурноста.

Кога се користат заедно, DHCP Snooping, Dynamic ARP Inspection и IP Source Guard формираат повеќеслојна безбедносна стратегија:

1. DHCP Snooping обезбедува точни IP-MAC записи и спречува DHCP spoofing.
2. DAI ја заштитува ARP комуникацијата од ARP poisoning.
3. IPSG го контролира IP сообраќајот и спречува IP spoofing.

Овие механизми заедно ја зголемуваат доверливоста, интегритетот и континуитетот на мрежната комуникација, минимизирајќи ризик од прислушување, неовластен пристап и манипулација со податоците. Тие се критични за корпоративни, академски и институционални мрежи каде што стабилноста и сигурноста се од суштинско значење.

Комбинацијата од DHCP Snooping, Dynamic ARP Inspection и IP Source Guard претставува интегрирана и ефективна безбедносна стратегија на Layer 2. Преку контрола и филтрирање на DHCP, ARP и IP пакети, овие механизми спречуваат DHCP и ARP spoofing, IP spoofing и други злоупотреби, овозможувајќи сигурна и континуирана мрежна комуникација. Во современите организациони мрежи, тие се неопходни за заштита на податоците и одржување на доверливоста и интегритетот на мрежната инфраструктура.

8.5. Безбедност на порта

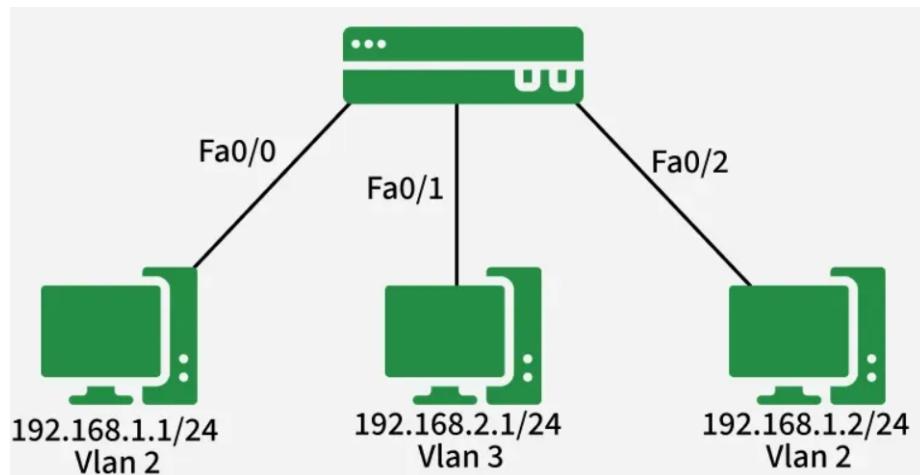
Port Security претставува клучен механизам на Layer 2 за заштита на локалната мрежа, кој овозможува ограничување на бројот на легитимни уреди кои можат да се поврзат на одреден switch-порт и спречува злоупотреби како MAC flooding, DHCP и ARP starvation. Кога Port Security се активира на портот, администраторот може да конфигурира максимален број на MAC адреси кои ќе бидат регистрирани на тој порт.

Секој нов уред кој се поврзува на портот се споредува со веќе регистрираните MAC адреси и, доколку бројот на уреди ја надмине зададената граница, switch-от презема однапред дефинирана акција. Овие акции можат да бидат различни: во режимот Protect, switch-от ги блокира пакетите од непознатите уреди, но продолжува да пропушта сообраќај од легитимните; во режимот Restrict, дополнително се генерира лог и аларм за администраторот; а во режимот Shutdown, портот се исклучува автоматски и останува во err-disabled состојба додека администраторот не го врати во функција. Овој механизам овозможува дека само одреден број на уреди може да комуницира преку портот, спречувајќи масовни напади или неовластено приклучување на мрежата. На пример, во корпоративна мрежа каде секоја работна станица се поврзува на switch преку индивидуален порт, ако е конфигуриран лимит од две MAC адреси по порт, напаѓач кој се обидува да приклучи свој лаптоп или да користи алатка за масовно испраќање MAC адреси ќе биде веднаш блокиран. Во режимот Restrict, switch-от ќе генерира известување, овозможувајќи на администраторот да интервенира навремено и да спречи потенцијални мрежни прекини. Еден од најчестите напади кои се спречуваат со Port Security е MAC flooding, каде напаѓач испраќа голем број пакети со различни лажни MAC адреси со цел да ја преплави CAM (Content Addressable Memory) табелата на switch-от. Кога CAM табелата се преполнува, switch-от не може да препознае легитимни MAC адреси и започнува да еmitува пакетите на сите порти, овозможувајќи на напаѓачот да прислушува сообраќај. Со ограничување на бројот на регистрирани MAC адреси, Port Security ја одржува стабилноста на CAM табелата и го спречува овој тип на напади. Дополнително, механизмот ги спречува DHCP и ARP starvation нападите, бидејќи само легитимните уреди добиваат пристап до DHCP серверот и ARP ресурси, додека сите обиди за масовно зафаќање на IP или ARP записи се блокираат. Port Security често се користи заедно со DHCP Snooping, Dynamic ARP Inspection и IP Source Guard за создавање на интегрирана повеќеслојна безбедносна архитектура. DHCP Snooping обезбедува доверливи IP-MAC записи и спречува DHCP spoofing, Dynamic ARP Inspection ја заштитува ARP комуникацијата од ARP poisoning, а IP Source Guard го контролира IP сообраќајот и спречува IP spoofing. Port Security ја дополнува оваа стратегија со физичко ограничување на бројот на уреди по порт и автоматска реакција при злоупотреби. Во ситуации каде многу уреди се поврзани на исти switch порти, како во канцелариски, академски или лабораториски средини, Port Security овозможува намалување на ризикот од MAC flooding, DHCP и ARP starvation, контрола на пристап до мрежата на Layer 2 ниво и поддршка за интегрирани безбедносни стратегии. Преку лимитирање на бројот на легитимни MAC адреси по порт, блокирање на непознати уреди и автоматска реакција при злоупотреби, Port Security спречува неовластен пристап и ја зголемува стабилноста и доверливоста на мрежната инфраструктура. Во комбинација со DHCP Snooping, Dynamic ARP Inspection и IP Source Guard, Port Security формира интегрирана, повеќеслојна стратегија за мрежна безбедност, која овозможува сигурна и континуирана комуникација, минимизирајќи ризик од напади и злоупотреби на локалната мрежа.

8.6. VLAN Сегментација

Современите локални мрежи се соочуваат со многу безбедносни закани на Layer 2 ниво, каде напаѓачи можат да пристапат до мрежата преку неовластени уреди, да измамат DHCP сервери, да ја зафаќаат ARP табелата или да ја преплават CAM меморијата на switch-овите. За заштита на мрежата и намалување на површината за напад, се користат повеќе интегрирани безбедносни механизми кои делуваат синхронизирано за да обезбедат контролиран и сигурен пристап. DHCP Snooping претставува една од основните техники која го штити мрежниот сообраќај од неовластени DHCP сервери и DHCP spoofing напади. Кога DHCP Snooping е активиран на switch, тој ги разграничува портовите на доверливи и недоверливи. Доверливи портови се оние преку кои легитимниот DHCP сервер испраќа DHCP Offer и DHCPACK пораки, додека сите останати портови се сметаат за недоверливи и на нив се блокира обид за испраќање DHCP пораки. Покрај тоа, DHCP Snooping овозможува rate limiting, со што се спречуваат DHCP starvation напади, каде напаѓач испраќа голем број DHCP Discover пораки за да ги зафати сите достапни IP адреси и да ја преземе улогата на DHCP сервер. На овој начин, DHCP Snooping обезбедува основна доверливост на IP-адресите дodelени во мрежата и го спречува масовното зафаќање на ресурси. Во комбинација со Dynamic ARP Inspection (DAI), се овозможува заштита од ARP poisoning, каде напаѓач може да практика лажни ARP пораки за да прислушува или изменува сообраќај. DAI користи доверливи записи од DHCP Snooping за да создаде табела со IP-MAC парови и проверува секоја ARP порака на мрежата. Доколку ARP пораката не одговара на доверливиот запис, таа се блокира, што значително ја намалува можноста за неовластена промена на ARP табелата и прислушување на сообраќајот. Дополнително, IP Source Guard (IPSG) ги контролира IP адресите кои се користат на недоверливи портови. Преку филтрирање на IP и MAC парови врз основа на DHCP Snooping табелата, IPSG спречува IP spoofing и гарантира дека само уреди со легитимна IP-MAC комбинација можат да испраќаат пакети преку одреден порт. Ова овозможува дополнителен слој на контрола на пристап, особено во средини каде има голем број на динамички IP адреси и повеќе VLAN сегменти. Port Security е дополнителна техника која ја ограничува физичката бројка на уреди на еден порт преку лимитирање на регистрирани MAC адреси. Ако бројот на поврзани уреди надмине зададената граница, switch-от може да блокира непознати уреди, да генерира аларм или да го исклучи портот. Ова спречува напади како MAC flooding, каде CAM меморијата се преплавува со лажни MAC адреси и switch-от почнува да еmitува пакетите на сите порти, овозможувајќи прислушување. Понатаму, Port Security го спречува и DHCP и ARP starvation, бидејќи само легитимните уреди можат да комуницираат со DHCP серверот и ARP ресурси. Конечно, VLAN сегментацијата ја намалува површината за напад преку логичко одвојување на мрежата на повеќе независни домени. Секој VLAN функционира како посебна логичка мрежа, каде уредите не можат директно да комуницираат со уреди од друг VLAN без посредство на routing или firewall. Со тоа, во случај на компромитирани уреди, напаѓачот не може слободно да се прошири во друг сегмент, што ја зголемува безбедноста на

корпоративната или институционалната мрежа. VLAN сегментацијата исто така овозможува примена на политики специфични за одделни групи на уреди, како QoS, firewall правила и ограничување на пристапот кон критични ресурси, а во комбинација со DHCP Snooping, DAI, IPSG и Port Security, создава интегрирана повеќеслојна одбранбена архитектура. Со овие механизми, секој слој на Layer 2 е заштитен: DHCP Snooping го контролира IP доделувањето и доверливите записи, DAI го штити ARP сообраќајот, IPSG го ограничува IP spoofing, Port Security ја контролира физичката бројка на уреди и VLAN сегментацијата го ограничува ширењето на потенцијални напади. Преку комбинација на сите овие техники, мрежата е заштитена од неовластен пристап, масовни напади, прислушување и злоупотреба на ресурси, што овозможува сигурна, стабилна и доверлива комуникација во корпоративни, академски или лабораториски средини. Примената на овие безбедносни техники е особено важна во денешните динамични мрежи, каде бројот на уреди и VLAN сегменти постојано се зголемува, а заканите стануваат се посложени и многубројни. Со правилна конфигурација и интеграција на DHCP Snooping, Dynamic ARP Inspection, IP Source Guard, Port Security и VLAN сегментација, администраторите можат да ја минимизираат површината за напад и да обезбедат континуирана, сигурна и ефикасна мрежна инфраструктура.



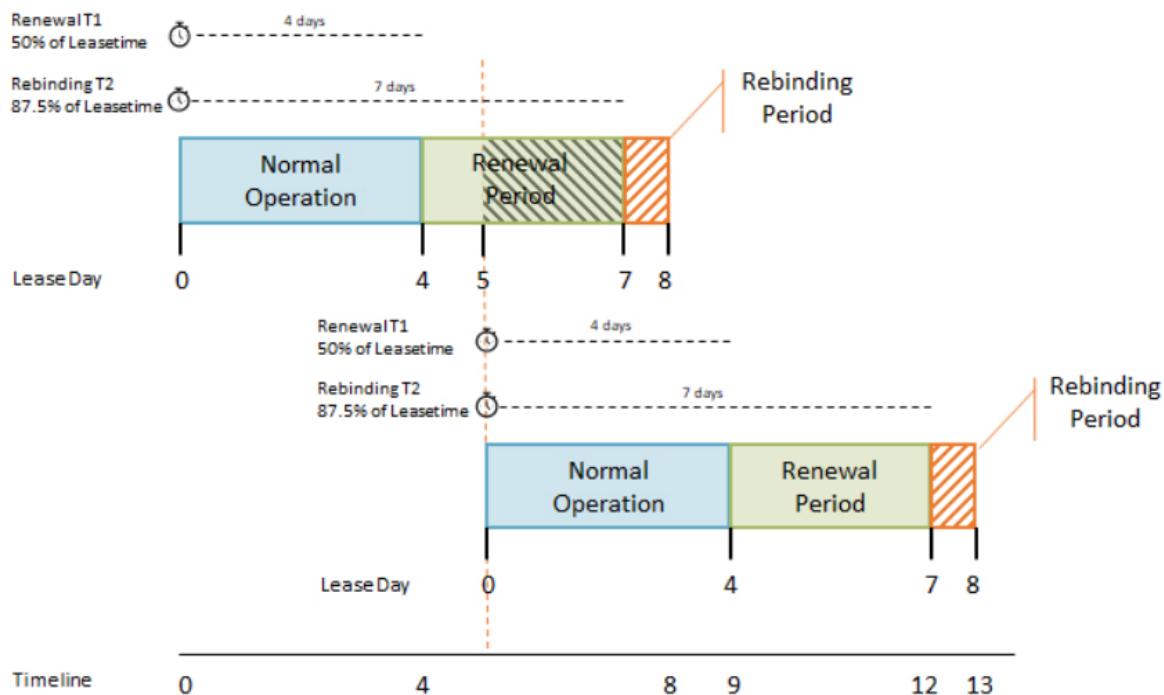
Слика 20. Сегментација во процес на заштита на DHCP со употреба на VLAN

8.7. DHCP Lease time

Контролирањето на времетраењето на DHCP lease претставува суштински механизам за управување и заштита на локалните мрежи, бидејќи директно влијае врз начинот на кој IP адресите се доделуваат, користат и ослободуваат од мрежните уреди. DHCP lease времето го дефинира периодот во кој една IP адреса е резервирана за одреден уред, по што уредот мора повторно да ја обнови или потврди таа адреса преку DHCP серверот. Овој процес овозможува автоматско и контролирано управување со ограничениот број IP адреси во мрежата и претставува важна точка на контрола од безбедносен и административен аспект. Без DHCP сервер и lease механизам, секој

уред би морал рачно да добие IP адреса, што не само што е неефикасно, туку и небезбедно во динамични мрежни средини. DHCP lease времето функционира како временска дозвола за користење на IP адресата, слично на адреса за живеење која е единствена и не смее да се користи од повеќе уреди истовремено. Во текот на животниот циклус на lease-от, уредот најпрво бара нова IP адреса, потоа ја користи во нормален режим, а на половина од времетраењето се обидува да ја обнови со цел да ја задржи истата адреса. Доколку DHCP серверот е недостапен, уредот влегува во фаза на повторно поврзување со било кој активен DHCP сервер, што овозможува континуитет на работата, но истовремено претставува потенцијална точка на ризик ако мрежата не е дополнително заштитена. Токму затоа, правилното дефинирање на DHCP lease времињата е од критично значење. Кратките DHCP lease времиња се особено погодни за динамични мрежи каде уредите често се приклучуваат и исклучуваат, како што се безжични мрежи, гостински VLAN сегменти, јавни hotspot-и и универзитетски кампуси. Во вакви средини, краткиот lease овозможува IP адресите брзо да се ослободуваат кога уредот ја напушта мрежата, со што се спречува исцрпување на DHCP pool-от и се намалува ризикот од DHCP starvation напади, каде напаѓач намерно зафаќа голем број IP адреси. Од безбедносна перспектива, ова значи дека компромитирани или сомнителни уреди немаат долготраен пристап до истата IP адреса, што ја отежнува нивната злоупотреба и го ограничува времетраењето на потенцијалниот напад. Истовремено, кратките lease времиња ја зголемуваат ефикасноста на безбедносните механизми како DHCP Snooping, Dynamic ARP Inspection и IP Source Guard, бидејќи IP-MAC binding табелите почесто се ажурираат и се намалува можноста за користење застарени или лажни записи. Сепак, прекумерно кратките lease периоди можат да предизвикаат зголемен DHCP сообраќај и административен overhead, па затоа мора внимателно да се балансира нивната должина. Од друга страна, подолгите DHCP lease времиња се попогодни за стабилни и контролирани мрежи, како што се корпоративни LAN средини, серверски сегменти и административни канцеларии, каде уредите ретко се менуваат и имаат постојана физичка локација. Во вакви случаи, подолгото времетраење на lease-от ја намалува потребата од чести обновувања, го намалува DHCP сообраќајот и ја олеснува мрежната администрација. Од безбедносен аспект, ова овозможува подобра конзистентност на IP адресите, поедноставено логирање и полесна анализа на инциденти, бидејќи активностите на уредите можат подолго време да се следат преку иста IP адреса. Сепак, ова носи и потенцијален ризик, бидејќи компромитиран уред може подолго време да ја задржи својата IP адреса доколку не се применуваат дополнителни заштитни механизми. Затоа, оптималната стратегија за управување со DHCP lease времињата не подразбира едно универзално решение, туку контекстуален пристап базиран на типот на мрежата и намената на уредите. Преку VLAN сегментација, можат да се применат различни lease времиња за различни мрежни сегменти, на пример кратки lease периоди за гостински и hotspot мрежи и подолги lease периоди за интерни и критични системи. Дополнително, мора да се внимава на големината на DHCP pool-от и секогаш да се остави доволна резерва на слободни IP адреси за да се избегне исцрпување на ресурсите. Во овој контекст, управувањето со DHCP lease времињата не е само административна поставка, туку активна

безбедносна техника која ја намалува површината за напад, го ограничува времетраењето на потенцијалните злоупотреби и ја зголемува стабилноста на мрежата. Во комбинација со статичко адресирање за критични уреди како рутери, switch-ови и мрежни печатачи, и со примена на DHCP Snooping, DAI, IP Source Guard и Port Security, DHCP lease механизмот станува дел од интегрирана повеќеслојна безбедносна архитектура. Ваквиот пристап овозможува подобра контрола, поефикасна администрација и повисоко ниво на заштита, што е од клучно значење за современите динамични и хетерогени мрежни средини.

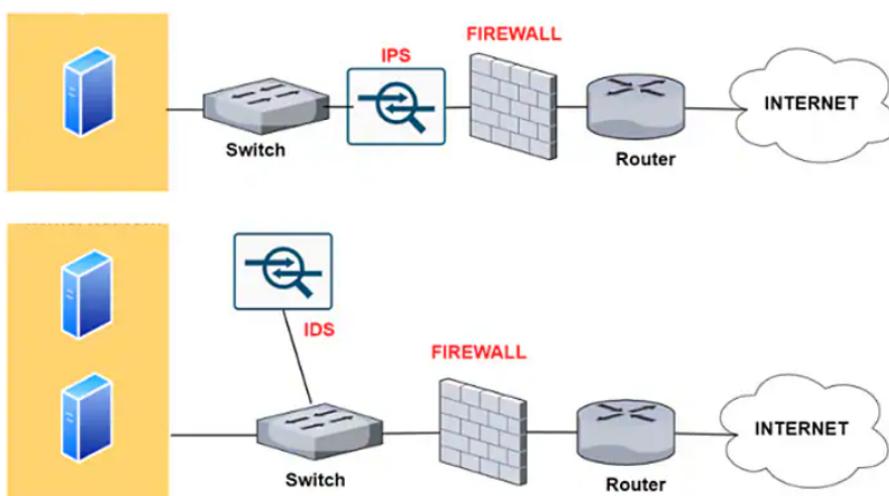


Слика 21. Временска разпределба - DHCP

8.8. Firewall и IDS/IPS мониторинг

Во современите корпоративни мрежи, firewall и IDS/IPS мониторингот претставуваат суштински елементи на сеопфатната стратегија за мрежна безбедност, бидејќи овозможуваат контрола, надзор и анализа на мрежниот сообраќај со цел навремено откривање, спречување и управување со безбедносни инциденти. Firewall-от е претставен како основна заштитна бариера помеѓу доверливите внатрешни мрежи и недоверливите надворешни мрежи, при што врз основа на однапред дефинирани правила активно дозволува или блокира сообраќај според изворна и дестинациска IP адреса, порти, протоколи и состојбата на конекцијата. Со ова се намалува површината за напад и се спречува неовластен пристап, но истовремено

firewall-от обезбедува и логирање на сообраќајот, што претставува вреден извор на податоци за анализа и форензика. Сепак, поради фактот што firewall-ите се базираат главно на правила и политики, тие не секогаш можат да ги детектираат сложените напади кои се одвиваат преку дозволен сообраќај, особено кога нападите доаѓаат од внатрешноста на мрежата. Тука значајна улога имаат системите за детекција и превенција на упади – IDS и IPS, кои ја надополнуваат функционалноста на firewall-от преку подлабинска инспекција на пакетите и анализа на однесувањето на мрежниот сообраќај. IDS системите се поставуваат надвор од директната комуникациска линија (out-of-band) и пасивно анализираат копија од сообраќајот, најчесто преку SPAN или TAP портови, со што не влијаат на перформансите на мрежата. Нивната примарна задача е да детектираат сомнителни активности и да алармираат кога ќе се забележи отстапување од нормалното однесување или совпаѓање со познати сигнатури на напади, како што се DNS poisoning, malformed пакети, port scanning или DoS активности. IPS системите, за разлика од IDS, се поставуваат inline, односно директно на патеката на сообраќајот, и имаат активна улога бидејќи не само што ги детектираат заканите, туку и автоматски реагираат со блокирање, прекинување или модифицирање на сомнителните конекции во реално време. Детекциските механизми кај IDS/IPS системите најчесто комбинираат сигнатурна анализа, која е ефикасна за препознавање познати напади, и анализа базирана на аномалии, која преку статистички модели и машинско учење дефинира нормално однесување на мрежата и ги открива отстапувањата од него. Иако аномалиската детекција е особено важна за откривање zero-day напади, таа носи и ризик од лажни позитивни аларми, што бара внимателно конфигурирање и континуирано прилагодување. Дополнително, IDS/IPS системите можат да бидат имплементирани како мрежни или хост-базирани решенија, при што мрежните IDS ги следат сите пакети што минуваат низ одреден сегмент од мрежата, а хост-базираните IDS ги мониторираат активностите на конкретен уред или сервер. И покрај нивната напредна функционалност, IDS/IPS системите се соочуваат со техники за избегнување на детекција, како што се



фрагментација на пакети, flooding напади, обfuscација на код и енкрипција на сообраќајот, што дополнително ја нагласува потребата од нивна интеграција со други безбедносни механизми. Токму затоа, интеграцијата на firewall и IDS/IPS со системи за

Слика 22. Дијаграм на споредба помеѓу IPS и IDS, со употреба на firewall

управување со безбедносни настани и инциденти (SIEM) има клучно значење, бидејќи овозможува централизирано собирање, корелација и анализа на логови и аларми од различни извори. Преку ваков интегриран пристап, безбедносните тимови добиваат целосна видливост врз мрежата, можност за побрза реакција и автоматизиран одговор на инциденти, како и подлабинска анализа на сложени и долготрајни напади. Комбинацијата од firewall, IDS и IPS, дополнета со напредни механизми за заштита од малициозен софтвер и експлоатација на ранливости, претставува основа на слоевита одбрана и Zero Trust пристап, при што секој сегмент од мрежата се третира како потенцијално недоверлив. Ваквиот холистички модел не само што ги намалува ризиците и последиците од сајбер напади, туку и овозможува поефикасно управување со безбедноста, подобра усогласеност со регулативите и зголемена доверливост и стабилност на целокупната мрежна инфраструктура.

9. Заклучок

Dynamic Host Configuration Protocol зазема централно место во современите мрежни инфраструктури, овозможувајќи автоматизирано доделување на IP адреси и ефикасно управување со мрежните ресурси во услови на зголемена динамичност и хетерогеност на уредите. Иако неговата основна функција е насочена кон поедноставување на мрежната администрација и подобрување на оперативната ефикасност, отсуството на вградени механизми за автентификација и контрола на доверливоста го прави протоколот подложен на различни безбедносни закани доколку не се имплементира соодветна заштита.

Анализата на придржните безбедносни техники, како што се DHCP Snooping, Dynamic ARP Inspection, IP Source Guard, Port Security, VLAN сегментација и управувањето со DHCP lease времињата, покажува дека безбедноста на DHCP не може да се постигне преку изолиран пристап, туку преку интегрирана и слоевита стратегија. Овие механизми овозможуваат прецизна контрола врз мрежниот сообраќај, верификација на идентитетот на уредите и ограничување на можностите за злоупотреба, со што значително се намалува ризикот од напади и нарушување на мрежната стабилност.

Може да се заклучи дека сигурното функционирање на DHCP претставува резултат на внимателно планирање, правилна конфигурација и континуирано следење на мрежната средина. Примената на соодветни политики и заштитни механизми не само што ја зголемува безбедноста на мрежата, туку и придонесува кон поголема доверливост, достапност и одржливост на комуникациските системи, што е од суштинско значење за современите организации и нивното дигитално работење.

10. Користена литература

[1] Geeks for Geeks, Dynamic Host Configuration Protocol (DHCP), достапно на:

<https://www.geeksforgeeks.org/computer-networks/dynamic-host-configuration-protocol-dhcp/>

[2] Efficient IP, What is DHCP? and Why is it important?, достапно на:

<https://efficientip.com/glossary/what-is-dhcp-and-why-is-it-important/>

[3] Akamai, How does Dynamic Host Configuration Protocol work?, достапно на:

<https://www.akamai.com/glossary/what-is-dhcp>

[4] PyNetLabs, DHCP with IPv6 (DHCIPv6) – Everything You Should Know, достапно на:

<https://www.pyenetlabs.com/dhcp-with-ipv6/>

[5] infoblox, DHCP and DHCIPv6:Commonalities and Differences, достапно на:

<https://www.infoblox.com/blog/ipv6-coe/dhcp-and-dhcpv6-commonalities-and-differences/>

[6] Geeks for Geeks, How DORA works?, достапно на:

<http://geeksforgeeks.org/computer-networks/how-dora-works/>

[7] IBM, Dynamic Host Configuration Protocol version 6, достапно на:

<https://www.ibm.com/docs/en/aix/7.2.0?topic=protocol-dynamic-host-configuration-version-6>

[8] LinkedIn, How Does DHCP Authentication Work?, достапно на:

<https://www.linkedin.com/advice/1/how-does-dhcp-authentication-work-can-you-f7o7e>

[9] Infoblox, DHCP Authentication Process, Infoblox Documentation, достапно на:

<https://docs.infoblox.com/space/NAG8/22252488/DHCP+Authentication+Process>

[10] GeeksforGeeks, DHCP Starvation Attack, достапно на:

<https://www.geeksforgeeks.org/ethical-hacking/dhcp-starvation-attack/>

[11] GeeksforGeeks, Rogue DHCP Server Attack, достапно на:

<https://www.geeksforgeeks.org/ethical-hacking/what-is-rogue-dhcp-server-attack/>

[12] Twingate, DHCP Spoofing, Twingate Cybersecurity Glossary, достапно на:

<https://www.twingate.com/blog/glossary/dhcp%20spoofing>

- [13] LinkedIn, A. Khan, *DHCP Spoofing Attack – Explanation*, достапно на:
https://www.linkedin.com/posts/adnan-khan-430625245_dhcp-spoofing-attack-what-is-dhcp-spoofing-activity-7383101459501850624-JLct/
- [14] F5 Labs, *The Dangers of DNS Hijacking*, F5 Networks, достапно на:
<https://www.f5.com/labs/articles/the-dangers-of-dns-hijacking>
- [15] Fortinet, *DNS Hijacking*, Fortinet Cyber Glossary, достапно на:
<https://www.fortinet.com/resources/cyberglossary/dns-hijacking>
- [16] Fiverr Resources, *Network Access Control (NAC) Diagram*, PDF документ, достапно на: https://fiverr-res.cloudinary.com/image/upload/f_pdf,q_auto/v1/attachments/delivery/asset/26023c1d0901d6dfbc0e9bd96d705454-1601878124/NAC%20Diagram.pdf
- [17] Wikipedia, *DHCP Snooping*, достапно на:
https://en.wikipedia.org/wiki/DHCP_snooping
- [18] CBT Nuggets, *What Is DHCP Snooping?*, достапно на:
<https://www.cbt nuggets.com/blog/technology/networking/what-is-dhcp-snooping>
- [19] FS Community, *What Is DHCP Snooping and How It Works*, FS.com Blog, достапно на:
<https://www.fs.com/blog/what-is-dhcp-snooping-and-how-it-works-1108.html>
- [20] NetworkLessons, *Dynamic ARP Inspection (DAI)*, достапно на:
<https://networklessons.com/switching/dai-dynamic-arp-inspection>
- [21] CablesAndKits, *What Is Dynamic ARP Inspection?*, достапно на:
<https://www.cablesandkits.com/learning-center/what-is-dynamic-arp-inspection/>
- [22] GeeksforGeeks, *Dynamic ARP Inspection*, достапно на:
<https://www.geeksforgeeks.org/computer-networks/what-is-dynamic-arp-inspection/>
- [23] Fortinet, *IP Source Guard*, FortiSwitch Administration Guide, достапно на:
<https://docs.fortinet.com/document/fortiswitch/7.2.10/administration-guide/183637/ip-source-guard>
- [24] PyNet Labs, *Port Security in Computer Networks*, достапно на:
<https://www.pynetlabs.com/port-security-in-computer-network/>
- [25] Huawei, *Port Security*, Huawei Networking Encyclopedia, достапно на:
<https://info.support.huawei.com/info-finder/encyclopedia/en/Port+Security.html>
- [26] Cisco Systems, *Port Security Configuration Guide*, Cisco Catalyst Series, достапно на:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-4SY/config_guide/sup6T/15_3_sy_swcg_6T/port_security.pdf
- [27] eSecurityPlanet, *What Is a VLAN?*, достапно на:
<https://www.esecurityplanet.com/networks/what-is-a-vlan/>

[28] GeeksforGeeks, *Virtual LAN (VLAN)*, достапно на:

<https://www.geeksforgeeks.org/computer-networks/virtual-lan-vlan/>

[29] ManageEngine, *DHCP Lease Time*, достапно на:

<https://www.manageengine.com/products/outils/tech-topics/dhcp-lease-time.html>

[30] Juniper Networks, *DHCP Lease Times*, Junos Documentation, достапно на:

<https://www.juniper.net/documentation/us/en/software/junos/subscriber-mgmt-sessions/topics/topic-map/dhcp-lease-times.html>

[31] LazyAdmin, *DHCP Lease Time Explained*, достапно на: <https://lazyadmin.nl/home-network/dhcp-lease-time/>

[32] Palo Alto Networks, *Intrusion Detection System (IDS)*, Cyberpedia, достапно на:

<https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids>